Theses and Dissertations 1. Thesis and Dissertation Collection, all items

2009-03

Simulation-based analysis and evaluation of tactical multi-hop radio networks

Smith, Howard D.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/4898

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SIMULATION-BASED ANALYSIS AND EVALUATION OF TACTICAL MULTI-HOP RADIO NETWORKS

by

Howard D. Smith

March 2009

Thesis Advisor:	John Gibson
Thesis Co-Advisor:	Gurminder Singh

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Simulation-Based Analysis of Tactical Multi-Hop Radio Networks		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Howard D. Smith			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

For many years, the technologies involved in the newest generations of tactical communication equipment have increased the reliability and security of tactical voice communications from the highest to the lowest levels of combat command. However, the complexities inherent to wireless data networks have prevented the reach of valuable data links from extending efficiently and reliably to the lowest levels of tactical command. This thesis attempts to quantify the performance of tactical data networks using existing technologies and currently deployed mobile wireless networking devices by analyzing the results of network simulations involving currently deployed devices. By quantifying these performance metrics and comparing them to previously collected simulation results involving experimental technologies, we hope to provide a mode of comparison that will accurately reflect the degree to which newer mobile wireless networking devices will benefit our operational forces.

14. SUBJECT TERMS Radio Networks, Multi-hop Networks, Computer Networks, Tactical Radio Networks, Software-Based Network Simulation, Network Analysis, SINCGARS, EPLRS, Cooperative Diversity, JCSS	15. NUMBER OF PAGES 125
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

SIMULATION-BASED ANALYSIS AND EVALUATION OF TACTICAL MULTI-HOP RADIO NETWORKS

Howard D. Smith
Captain, United States Marine Corps
B.S., United States Naval Academy, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
March 2009

Author: Howard D. Smith

Approved by: John H. Gibson
                 Thesis Advisor

                 Gurminder Singh
                 Co-Advisor

                 Dr. Peter J. Denning
                 Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

For m any years, the technologies involved in the newest generations of tactical communication equipm ent have in creased the reliability and s ecurity of tactical v oice communications from the highest to the lowest levels of combat command. However, the complexities inherent to wireless data networks have prevented the reach of valuable data links from e xtending efficiently and reliably to the lowest levels of tactical comm and. This thesis attempts to quantify the performance of tactical data networks using existing technologies and currently deployed mobile wireless networking devices by analyzing the results of n etwork s imulations inv olving cu rrently deployed devices. By quantif ying these performance metrics and comparing them to previously collected simulation results involving experimental technologies, we hope to provide a mode of comparison that will accurately reflect the d egree to wh ich newe r mobile wireless netw orking devices will benefit our operational forces.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OBJECTIVE

Our objective for this thesis is to model a variety of realistic network simulations, which demonstrate the performance of current ly deployed wireless mobile networking devices, in a manner that is consistent with current tactical data network loads. We wish to demonstrate each network's ability to s upport the demands of a variety of different data traffic densities, and then compare the performance of each model to the results of a model used in previous thesis research simulations, involvi ng an experim ental communications device that implem ents som e e merging wireless networking technologies. Most of our sim ulations will be roughly based on the sim ulations performed in [1], and after our analytical baseline is established, we will then discuss any performance gains or losses f ound within each type of netw ork and explore the reasons for any divergences.

The main contribution of this research will be the quantificati on of specific data networking performance metrics for legacy m obile wireless networki ng devices, and the comparison of these res ults to the already quantified performance results from [1]. Our intent is to provide a more accu rate understanding of the actual de gree to which newer wireless mobile networking technologies can benefit our operational forces.

B. WHY DATA AT LOWER TACTICAL COMMAND LEVELS

The ability to provide data services to the lowest leve ls of tactica l com bat commands has existed for decades. However, the low available bandwidth and difficulty of i mplementation of the data services with in currently deployed devices has severely limited the operational incorpor ation of data services outside the stationary comm and center. The problem with many of the radios being used by our military is that they were designed with voice communications as the primary focus, with data capabilities added as an inefficient secondary capability.

1

The development of improved wireless data networking technologies has enabled the crea tion of certain wireless n etworking devices that could effectively extend significant infor mation flow outside of th e stationary comm and center and allow unit commanders to share greater quantity and better quality of information with the ir lower (typically highly mobile) levels of command.

For exam ple, with m ore effective data network links, it would be possible to quickly provide significantly m ore detailed targeting information (i.e., a photograph or live streaming video) to the sm aller mobile units, which would re duce the probability of them targeting inappropriate buildings, vehicles or people.

Although the benefits of increa sed tactical data capabilities have been recognized for a long time, it has not been until recently th at the technologies that promise to fill this communication gap have begun to m ature to the point of possible im plementation. With a relatively recent increase in the amount   of c ommercial dem and for m obile wireless voice and data services, we have seen an   unprecedented growth in the developm ent and refinement of m ore capable and reliable m obile networking technologies. Incorporating these new technologies into our tactical comm unication architecture will be crucial to our military's a bility m aintain our tech nological ad vantage, an d it will gre atly inc rease our tactical commanders' ability to more accurately ascertain real-time battlefield conditions, in order to more quickly m   ake inform ed decisions during their ex ecution of com bat operations.

C.   RESEARCH QUESTIONS

1. W hat kind of data traffic is required by units functioning at the lower tactical levels of command?

2. W   hat are th e cap abilities an d lim itations of curren tly f ielded wireles s networking devices?

3. How does the ability of currently   available m obile networking devices to handle various types of data network traffic lo ads compare to that of devices using newer types of wireless networking technologies?

4. What, if any, improved capabilities should be achieved by future devices, and are these improvements significant enough to justify the fielding of new equipment?

D. ORGANIZATION

In Chapter II, we will provide an overview of the seven-layer OSI Service Model, as presented in [14], with an emphasis on the characteristics of the data link layer, mobile multi-hop networks and some of the issues that make them so challenging to implement, and on one of the newly implemented technologies that holds some promise of overcoming some of the limitations of wireless networks at the link layer, which were previously modeled and analyzed in [1].

In Chapter III, we will explain the general functionality of the different radios to be modeled and the limitations of each radio's ability to provide the types of data network capabilities really needed at the tactical levels.

In Chapter IV, we will explain the characteristics and limitations of the Joint Communications Simulation System network simulation software we will use to analyze and evaluate the effects of various types of network traffic across existing tactical radios.

In Chapter V, we will compare the results of our simulations with those obtained from simulations involving a specific prototype device that was modeled under similar scenarios in previous thesis work.

In Chapter VI, we will summarize the overall comparisons between the performances of each of the simulated radios and make recommendations for future research related to our results.

THIS PAGE INTENTIONALLY LEFT BLANK

II.   BACKGROUND INFORMATION

A.   OSI SERVICE MODEL ARCHITECTURE OVERVIEW

In order to provide some kind of structure to the development of different network protocols, current netw orking developers usually operate with in the boundaries of commonly accepted service m odel arch itectures. One of the m ost comm on network service models is the se ven-layered Open Systems Intercon nection (OS I) serv ice b ased architecture paradigm.
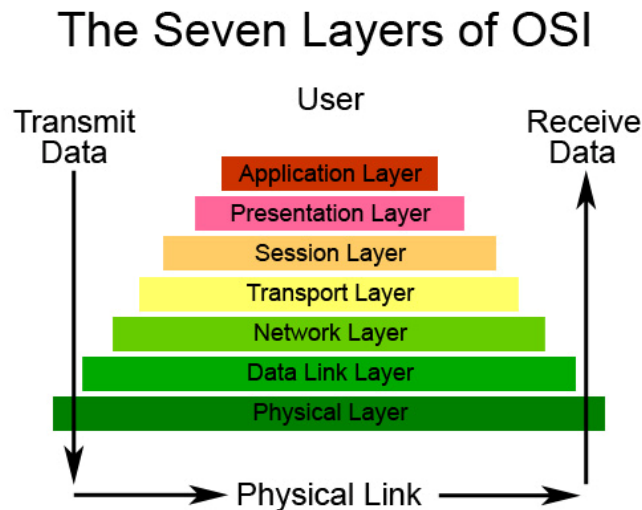
Figure 1.   7-Layer OSI Model (From University of Washington website).

As shown i n Figure 1, this architecture   divides all netw orking protocols into layers, or groups of services, based on the specific functions they help perform during the data networking process. Processes at each layer of service communicate with each other and work in conjunction to provide specific serv ices to the layer above it. Each layer can only use the service s provided by the layer be   low it, and this unif orm f low of utility allows the functions perform   ed within each   layer to operate independently of the functions performed within any of the other layers. This   modularity of function allows network designers g   reater flexib ility in ho   w they choose to co   mbine different

implementations of services perform ed at each layer, with out having to worry about a single change at one layer causing each of the other layers to stop functioning.

The first tw o layers, the physical and da ta link layers, and the functions they perform are of particular interest to the ana lysis performed in this the sis, since it is the establishment of reliable and efficient wireless data link connections that present the most significant challenges to the creation of data networks across mobile wireless nodes.

1. Physical Layer

The physical layer encompasses all protocols and functions perform ed by the physical medium by which a si gnal carrying network informa tion is accomplished. This includes, bu t is not lim ited to rad io waves traveling through the air, analog waveforms traveling across copper wire, or discrete light waves traveling across fiber optical wires.

For the purposes of this thesis, all physical layer transmission simulations will be radio waves being transmitted through the air between like communication nodes.

2. Link Layer

The link layer encom passes all protocol s and functions perfor med between two communication nodes immediately before se nding and immediatel y after receiving frames across the physical layer. T he link la yer's main purpose is to forward a networ k layer datagram through whatever types of transmission links exist along the path from the transmission's sender to its destination. If there are different types of links along this path, th en the link layer will perform different tasks accord ingly, in o rder to accommodate the needs of each type of link. The different tasks perform ed at diffe rent types of links are transparent to the processes running at the network layer.

Some common tasks perform ed by pro cesses running at the link layer are encapsulation, contro lling overall lin k access, ensuring relia ble delivery, contro lling the flow of fram es across each link, and erro r de tection/correction of each fram e. All of these pro cesses work to wards the c ommon purpose of ensuring tha t e ach tran smitted frame is reliably received by each communicating node without errors. It also attempts to

ensure that each transm ission does not in terfere with the transm issions of other no des communicating across the sam e physical m edium, in a m anner that perm anently denies another sender access to network resources.

It is the f unctions performed at the link layer that create the m ost unique types of complexity, especially when there are many c ommunication nodes attem pting to share access to the sam e wireles s trans mission medium. W ireless links are m uch more susceptible to signal errors caused by th e surrounding environm ent (electrom agnetic radiations, com peting communication tr ansmissions, m ultipath inte rferences, etc.), so effective error detection and correction prot ocols are m uch more im portant, and can be significantly more difficult in wireless networks than in wired networks.

There are also generally less wireles s bandwidth resources a vailable to m eet the throughput needs of host applications, so an application (or a suite of m ultiple applications) that m ay run very well on a wired network, may perf orm poorly when run across a wireless m edium. While wired networks can always add more wires to increase the number of channels available for signal transmission, wireless networks are limited to the use of a fixed am ount of available rad io frequency spectrum. It is because of these difficulties that the f unctions pe rformed at the link lay er a re the m ost relevan t to the different communications nodes evaluated later in this thesis, and are discussed in more detail below.

a. Encapsulation

Encapsulation is an important con cept, because different types of networked devices m ay perform this task very differently from one another. Encapsulation is used by the link layer to create a data fram e that is form atted appropriately for transm ission directly acr oss the physical layer data transm ission medium.

Services b elonging to the link lay er will receive a datag ram from the network layer and add an additiona l header and trailer to it, in order to create a properly formatted link layer frame. This means that the actual frame being transmitted across the physical m edium is different from the datagr am that will ultim ately be received by the

7

different layer protocols running on the receiving devices. This is because the information required to forward each frame across each communication link is not a concern of the higher layered protocols, so it is not generated or shared outside of the link layer. Also, since the size of each encapsulated frame can have a significant effect on throughput and retransmission requirements for each frame, some link layer services may divide the network layer frames into smaller sized fragments, which will each be encapsulated and transmitted across the physical layer separately, only to be pieced back together at the receiving node. The smaller each fragment is, the more likely it will be able to reach its destination without errors from signal interference.

However, it is not always the case that smaller fragments are desirable for a given data link. If the same amount of overhead is required to forward each fragment, then with an increased quantity of fragments being forwarded, there will be more total overhead introduced across each link. This will decrease the overall throughput of a data link. So, smaller fragment sizes may not be suitable for hosts that require links with higher throughputs. These kinds of considerations create complexities for network managers, who must balance the throughput needs with the acceptable level of errors/retransmissions based on the needs of the supported hosts.

b.   *Error Detection/Correction*

Error detection is an important function performed by the data link layer protocols because it is typically at the physical layer where most frame errors occur. This is especially true for networks operating across wireless communication links, since the quantity and types of interference inherent in wireless waveform propagation far exceed the types of interference affecting wired waveform propagation.

Error detection is typically performed using a checksum value or a Cyclic Redundancy Check (CRC) included in the trailer of the link layer frame, which is created by the transmitting node for every unique frame transmitted, and used by the receiving node to validate the integrity of each received frame. If an error is detected, the frame can be retransmitted at the link layer level, without requiring the higher level protocols to detect and retransmit the erroneous frame.

8

Alternatively, m any link protocols use types of forward error correction schemes, such as fountain coding, which not on ly allow the host to de tect an error in a corrupted fragment, but also allow potential co rrection of these fragm ents. This m ethod could be desirable over more sim ple error detection schemes, since it elim inates the need for these co rrupted fragments to be retran smitted across th e link. W hile this m ethod of error correction requires som e additional pr ocessing cap abilities on behalf of the receiving h ost, th e m ain drawback to th e us e of these schem es is in the additional overhead required for their implementation, and the decrease in link throughput it causes.

c.   *Media Access Control*

Media Access Control (MAC) is a prot ocol that attem pts to govern the manner in which each networked communication node accesses the transm ission medium. Various types of MAC protocols have been developed that attem pt to perfor m this task in different m anners. The m ain goal of a MAC pr otocol is to ensure th at each node attached to the network is allowed to transm it its si gnal across the transm ission medium as quickly as possible, while producing m inimum interference with the transmissions of other nodes attempting to access the same transmission medium.

Balancing the desire for high throughput at each no de with th e minimization of overall transm ission collisions is espec ially challeng ing when working with wireless networks. Si nce two-way wireless links are half-duplex by nature (assuming all nodes are only communicating acro ss a single channel), wireless networks cannot effectively use the m ore efficient MAC protocols that are so common in the full-duplex wired networks.

Additionally, unlike wired networks, there is no guarantee that ev ery wireless node can detect the transm issions of all other nodes in the sam e wireless network. A s shown in Figure 2, the "hidden node" problem, can rend er an intermediary node incap able of relay ing eith er on e of th e tw o tran smitting node's transm issions. If both node A and node B are not within rang e of each ot her, then th e Hub node m ay receive both signals at the sam e time and not be able to understand either one of t hem.

9

This m eans that it is p ossible for two nodes to attem pt to access th e sam e network resources at the sam e, without ever realizing that their transmissions are interfering with each other.
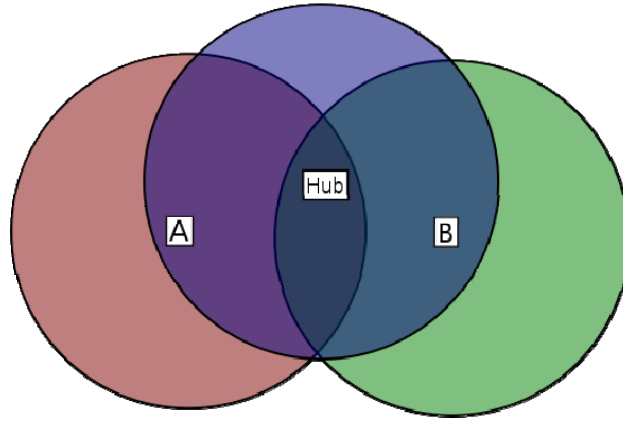
Figure 2.   Hidden Node Problem (From Wikipedia.org).

B.   MULTI-HOP MOBILE NETWORKS

A m ulti-hop m obile network is n etwork composed of more than two m obile nodes, where it is possible fo r two of the nodes within th e network, which are not in direct contact (i.e., they are out of t ransmission range of each other), to send and receive transmissions between each other through sep arate nodes that belon g to the same network.

1.   How Multi-hop Networks Work

In a multi-hop network, in order for a signal packet to travel from the originating node to the destination node it m ay be necessary for the packet to trav el throug h more than one ho p or tran smission time slot. In o rder to accom plish this, the packet m ust be relayed through a separate node (or multiple separate nodes) that acts as a relay.

For exam ple, in Figure 3 the center node, whose transm ission radius is represented by the red (center-m ost) circle, is not within transm ission range of the

10

leftmost node, whose transmission radius is represented by the blue circle. In order for a packet to travel from the center node to the leftmost node, it must be relayed through the node whose transmission range is represented by the yellow (upper-center) circle. The yellow node acts as a relay node that belongs to the same network as the other two nodes, but is neither the originator nor final recipient of the packet. Thus, since the source and destination nodes are separated by more than a single hop and can still communicate with each other, it is considered to be a multi-hop network.
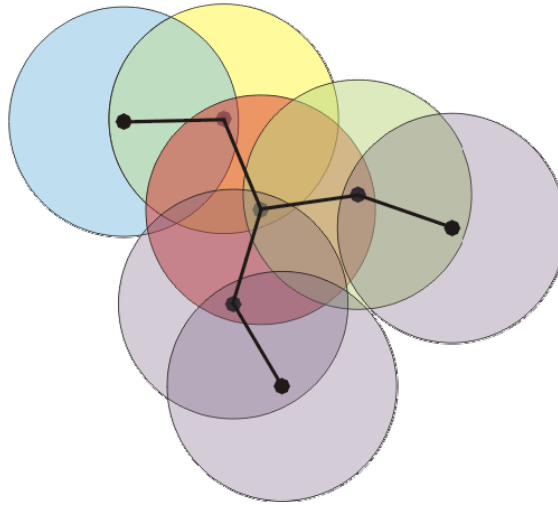
Figure 3.   Multi-hop Network Node Diagram (From RWTH-AACHEN University website).

Multi-hop networks can be very useful when a particular node needs to communicate with a node that is outside of its own transmission range, and can greatly expand the overall communications range of any node within a single multi-hop network. As long as the originating node is within range of another node that is either linked directly or indirectly with the destination node, it can still send the packet with a reasonable expectation that it will eventually arrive at the desired destination.

2. Complexities Inherent To Multi-hop Networks

a. *Infinite Loops*

In a single-hop or infrastructure-based wireless radio netw ork, if a node receives a packet that is destined to a different node it will simply ignore it. In a wireless multi-hop network, the receiving node may relay th e packet in an attempt to deliver the message to som e distant recip ient that m ight not be within range of the transm ission's originator. If there are more than one relaying nodes, there is the possibili ty that these intermediary nodes will cont inue to exchange these retransm issions indefinitely, producing a kind of infinite r eceive-retransmit cy cle. This will not only reduce the available bandwidth to all nodes within range of these transm issions, but will unnecessarily tie up processing resources of each node involv ed in the loop. This is similar to is sues exper ienced in ear ly Ethe rnet networks, and was solved by assigning each packet a TTL number, which is decrem ented by each routing node that retransm its the packet. This sam e type of solution can be im plemented in a m ulti-hop wireless by introducing a maximum hop limit for each transmission.

Another m ethod of m itigating infinite loop s is the im plementation of a controlled network flooding scheme. In this scheme, each packet received by a node, but is not destined for that node, is relayed once and only once. This ensures that each packet will be transmitted across the entire area of network coverage, but avoids the potential for infinite loop s, since a n ode encountering th e sam e packet more than o nce will s imply drop it. The main problem encountered in this type of scheme is in the implementation of a m ethod that allows each node to accurately distinguish b etween copies of previo usly encountered packets and packets that it has not yet processed.

Controlled flooding can be i mplemented in two ways: it can use the packet head er to sto re the accum ulated rou ting data created as each p acket is relayed through the network, or it can req uire each node to cach e packet data locally, and compare the cached data to each received pack et. In h eavily trafficked networks, the additional overhead of adding rou ting data to each packet header m ay be undesirable due to the poten tial for in creased netwo rk congestio n. Additio nally, ask ing each node to

maintain a cache of previously seen packet s increases the s torage and pro cessing burden on each node device, which m ay pl ace an undesirab le am ount of strain on the device's power and hardware resources.

b. Hop Limits

Placing a maximum limit on the number of hops a packet can travel before being discarded m ay elim inate the possibility of infinite transm ission loops form ing between two nodes, but it also introduces limitations to the overall coverage area of the network, so this lim it must be chosen careful ly. If the hop lim it is too low, this could significantly reduce th e transm ission area c overage benefits gained by im plementing a multi-hop n etwork. If the hop lim it is too h igh, there can still be sig nificant drain on network and node resources, sim ilar to that incurred from infinite transm ission loops. Therefore, the m aximum hop lim it m ust be set to a level that eff ectively balances the needs to the network users and the lim itations of the network nodes. At a m inimum, the hop limit should be at least slightly greater than the expected diameter of the network. I f it is sm aller than the ne twork diameter, th en it is possible for a packet to be dropped before it ev en has a chance to trav el far enough reach its destinati on. If the hop lim it is significantly grea ter tha n th e network diam eter, then p roblems with creating netw ork congestion may occur.

c. Reduced Bandwidth

All wireless nodes utilize the same physical transm ission m edium to transmit any type of network traffic. So, i f each node spends tim e retransmitting traffi c they did not originate, then it m eans they m ust spend less tim e transmitting their own traffic. The necessary o verhead of retransm ission traffic in multi-hop n etworks takes up bandwidth that cannot be used by other nodes to initiate their own tr ansmissions, so this potentially e ffectively r educes the b andwidth available to any one node, assum ing it is not the only node allowed to originate transmissions.

When a net work node transm its a signal destined to another node that is more than o ne hop away, the trans mitting node m ust wait at a m inimum for the closes t

relaying node to retrans mit the signal, before transmitting its next segment. If this does not happen, the second transmission will interfere with the relaying of the first.

In som e cases, if a network has a m aximum hop count of n, each transmitting node will wait n-1 time slots between transmissions, in o rder to ensure that no collisions occur between its next transm ission and the transm issions of nodes that are still relaying the original message. This type of transmission delay is used by the EPLRS device discussed in later chap ters, and really only benefits mobile networks whose nodes may shift between being tightly bunched and sp read far ap art, as it wo uld ensure that collisions are not cause by relay transm issions when all network devices are within transmission range of each other. W hile this m ay hel p decrease the chance of interference between transmissions, it also decreases each no de's available throughput to $1/n$ of the total number of time slots.

d.   Additional Processing Required

While the implem entation of a wireless m ulti-hop network seem s simple in theory, there are certainly greater pro cessing and buffering requirements introduced by the need for each individual network node to perform a greater number of tasks related to processing each receiv ed transm ission. E ach node has the addition al com putational burden of needing to anal yze each received transm ission and recognize if that transmission is destined to itself or to a nother node, and perfor m some form of queuing process for the message to be retransmitted and, then retransmit it at the same time that it may be trying to transmit its own messages. While these tasks are no different than those of routers in a wired network, in a wireless network all hosts must perform these actions. These actions may have additional power requirements for which existing hardware is not well suited and could introduce m obility restrictions by requiring la rger batteries (m ore weight) or less distance between transm itting nodes (lower transmission power), in o rder to compensate for greater energy demand on each node.

C.   COOPERATIVE DIVERSITY

Cooperative Diversity is a technique used   within wireless data networks where multiple quasi-simultaneously received transmission signals can be combined, in order to increase the accuracy of a signal that m   ay otherwise b e unreadable due to signal attenuation or interference between the separa te signals. Since the previous thesis work being used as a com parison to the sim ulations created in this thesis utiliz ed a wireless network device that im plemented some form of this capability, we have included a brief explanation of this relatively new wireless networking capability.

1.   How Cooperative Diversity Works

According to conventio nal wireless networ king schem es, if a wireless receiv er detects multiple signals being transmitted across the same channel, the node may have to ignore what it receives and consider the com bination of both transm issions to be simple noise on the channel, because it is unable to distinguish one signal from the other. Using cooperative diversity, a wireless receiver can recognize multiple occurrences of the sa me transmission, even if they are slightly out   of synch with each ot her, and com bine both occurrences into a single amplified signal. Es sentially, this capability mimics the use of multipath signal combinations, or special diversity, where a node rece ives several signals overlapping in time that share the sam e source. These signals arrive at slightly different times due t o the difference in path lengths caused by reflections or refractions of the signals. Th e key difference with cooperative   divers ity is that the m ultiple received signals are actually received   from different transm ission sources (nodes) that each received and relayed th e sam e source packet, without m odification (save for identical time-to-live changes and resulting integrity check (CRC) modifications, if used) resulting in the multiple receptions. The implementation of this capability, generically modeled by [1], is paten ted by TrellisW are, Inc., which provides a m ore detailed description of their technology in [4]. The general concept is described below

As shown in Figure 4, when S transm   its a signal, the signal can be received by any number of R_n stations. If m ore than one of the R_i station attempts to relay the s ignal to D, then D will receive multiple instances of the same signal originated by S. Since the

15

distance between each R $_i$ station an d both S an d D are s lightly different, each of th e Ri$_n$ station's transmission will arrive at D at slightly different times. Multiple versions of the same signal can occur in networks where m ultiple nodes act as transmission relays for another node, or if a single node 's signal is partially reflec ted off of a physical terrain object and redirected in the same direction as the signal's intended receiver.
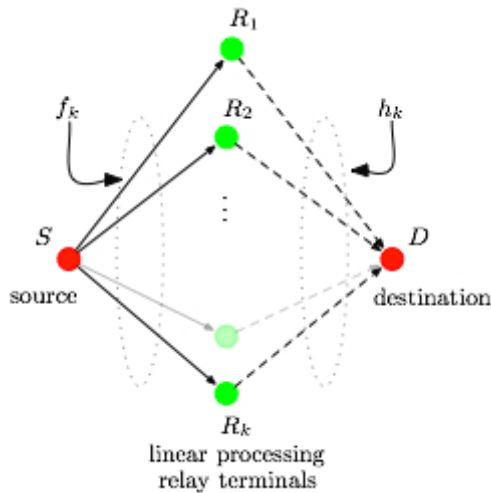
Figure 4.   Cooperative Diversity Model (From Swiss Federal Institute of Technology Zurich website).

2.   Why Cooperative Diversity Is Useful

Cooperative diversity can be particularly usef ul for netw orked nodes that are operating within a highly reflective (i.e., urba n or extrem ely rocky) environm ent. The wireless node evaluated in [1] implem ents a version of cooperati ve diversity, in an attempt to increase the reliability of each trans mitted signal and to alle viate the po tential confusion caused by a single node's reception of multiple identical signals from separate nodes retransmitting identical signals from a more distant signal originator. Since each of these nodes will relay a transm ission for which they are not the in tended recipient, there is a high p otential for m ultiple n on-destination nodes to receive a transm ission at approximately similar times, and then retransmit them such that identical signals arrive at the distant destination node at close to id entical tim es. If there was no type of

cooperative diversity imple mented at the re ceiving node, then in any network that consisted of m ore than two nodes, it w ould be very likely that m ost received transmissions would be regarded as interfer ence and discarded, because of the difference in the timing of the multiple relayed signals.

While data networks in gener al are ex tremely com plicated entities, m obile wireless networks intr oduce additional com plexities th at f urther com plicate the deployment of effective wire less data communications. U nderstanding the different levels of network functionality is crucial to both understanding the problems encountered with these networks and the ben efits and limitations to proposed solutions to each problem.

The following chapter discusses three mobile wireless network devices. The first two are currently deploy ed wireless communication devices, one of which provides only simple mobile single-hop wireless data links and the other provides an early version of a mobile multi-hop wireless data link network. The third device is not currently deployed, but it uses som e e merging m obile wire less communication technologies, including cooperative diversity, to provi de enhanced m obile wirele ss communications that could greatly increase the tactical communication capabilities over currently deployed devices.

THIS PAGE INTENTIONALLY LEFT BLANK

III.   ANALYSIS OF DEVICES DISCUSSED IN SIMULATIONS

A.   SINCGARS

Since its initial fielding in 1993, the Si ngle Channel Ground and Airborne Radio System (SINCGARS) has been th e prim ary t actical com munications device of the US Military. While three of its six radio terminal versions support data communication links, this radio was designed and deployed primarily as a voice communications device.

The SINCGARS radio is worth m entioning in this thesis because of its prominent presence within all lev els of tactical co mmand and con trol architectures. This radio provides both data and voice communication serv ices, but its low data rate lim itations essentially disqualify it from being a ca ndidate for running the same suites of data network applications as the EPLRS radio (described later in this chapter) or as more data-capable emerging m obile wireless networking devices. Its general data characteristics and network sim ulation perform ances are includ ed here for com pleteness, and because these capabilities are not entirely without benefits.

The SINCGARS radio generates frequency   modulated (FM) signa ls within the low VHF fr equency range of 30-87.975 MHz, and can be used in either single frequency or frequency hopping modes. The data capable versions of the radio term   inal can transmit in five different data modes, ranging from 600 bps to a maximum data rate of 16 Kbps. Its data tran smissions are lim ited to a single FM analog data stream, and the radio terminal has no built-in error correction capabilities. Since this type of data signal is very susceptible to signal interference, when a SINCGARS radio terminal is transmitting at its maximum data rate of 16 Kbps, its line-of-sight transmission planning range is cut almost in half, as indicated in Table 1. This is   becau se the higher throughput analog sign al is more susceptible to noise introduced into th e transm ission at the higher power levels required to travel the longer distances. Th e SINCGARS does not include any kind of embedded MAC protocols, so an y network acce ss control m ust be controlled at th e application layer. S ince the SINCARS is typically a single-hop communication device,

19

this would severe ly res trict the tac tical commander's ability to m aneuver units in a manner that ensured continuous data connectivity via SINCGARS data links.

TYPE RADIO	DATA RATE	RF PWR	PLANNING RANGES*
MANPACK/ VEHICULAR	600 - 4800 bps 16000 bps	HI HI	3 km - 5 km 1 km - 3 km
VEHICULAR ONLY	600 - 2400 bps 4800 bps 16000 bps	PA PA PA	5 km - 25 km 5 km - 22 km 3 km - 10 km

* Vehicular radios only.

Note: Planning ranges are based upon line of sight and are average for normal conditions. Ranges depends on location, sighting, weather, and surrounding noise level, among other factors. Use of OE-254 antenna will increase ranges for both voice and data transmissions. Enemy jamming and mutual interference conditions will degrade these ranges. In data transmissions, use of lower data rates will increase range.

Table 1.   SINCGARS Data Transmission Maximum Planning Range (From [11]).

Even if a re transmission site wer e u sed to supp ort the se lin ks, sim ilarly to how analog voice communication rang es are extended in SINCGARS networ ks, it would still not help extend these ranges. Since SINC GARS retransm issions are accom plished by connecting two SINCGARS radios by a cable and having one radio autom atically relay any signal received by the other, th e retransmitted signal is sim ply an amplified version of the original analog signal. Since the ra dio does not process and regenerate the data packet being relayed, the retransmitted signal would still contain any degradation, such as interference from other signals or noise intr oduced by environmental factors, which keep the data from being understood by its destination.

Despite these range lim itations, point-t o-point data applications using the SINCGARS have existe d for some time. Since there are no data generating applications organic to the SINCGARS radio term inal, the data transmitted across a SINCGARS data link m ust be generated by an externally connected device. Also, be cause there is no routing capability with in the device, data links ar e typically lim ited to one-hop communications. Som e specialized data gene ration devices take advantage of the data capability of this radio, but only allo w single-hop data communi cations between SINCGARS radios and limit data traffic to simple, preformatted text messages.

20

A regular personal computer (PC) can be connected to the SINCGARS radio terminal via a specialized data cable, which connects the radio terminal's data port to the computer's serial port. In this configuration, each data transmission can only be received by a similarly configured SINCGARS radio terminal with an attached PC. There is no traffic limitation to the types of files sent across such a link, but because of the link's small throughput (16 Kbps), it would not be well suited for applications with heavy traffic requirements. The requirement of additional data equipment also places increased weight and physical space restrictions on users wishing to transmit data using SINCGARS radios.

Since the SINCGARS radio was designed as a voice-centric physical layer communication device, it does not contain any preprogrammed data routing or MAC protocols for the use in creating multi-node data networks. As a result, it is up to the attached data device to perform data routing and MAC functions for the network.

As explored in [6], it is shown that it is possible to implement more modern types of data networks, such as mobile ad hoc networks (MANETS) between multiple devices, using the SINCGARS radio terminal as the physical layer device. This was accomplished using the data cable to connect a PC to the SINCGARS radio terminal, and running software implemented link and network layers that receive transmitted data packets and either accepts them, passing them to the appropriate application or retransmits them to other SINCGARS radios.

This application allows the radio to retransmit a newly created version of the data packet (without any noise that may have interfered with the initial signal), instead of merely relaying an amplified version of the same signal. This method of packet retransmission could overcome some of the range limitations for retransmitted data signals in a SINCGARS network, by eliminating any noise that may have been introduced to the original analog signal.

Another development of technologies available for using SINCGARS radios for data traffic is the Internet Controller (INC) circuit card that can be installed in the vehicle amplifier adapters (VAA) for the newer versions of SINCGARS radios. This device acts

21

as a basic IP router that allows for the routing of data to other SINCGARS radios, EPLRS radios and other PCs connected to the INC. It allows an extern al da ta device to be connected via an included Ethernet port and it is compatible with any device that supports 802.2 and 802.3 protocols. It also provides improved forward error correction (FEC) capabilities and claim s to increase the pla nning range for its data links through digital conversion and retransm ission. However, th e INC is not dism ountable, so it does not provide data capabilities to foot mobile troops, and it does not increase the throughput of a SINCGARS data link. In fact, where it is implemented, the overhead required for FEC will actually reduce the amount of usable data throughput.

Regardless of the m ode of data tran smission across a SINCGARS data link, the data rate limitations of such im plementations still restrict communications to da ta traffic with very sm all throughput requirem ents, su ch as sending sim ple text m essages and would not provide sufficiently large transmission channels for the use of VoIP services or the exchange of larger data files.

B.   EPLRS

The Enhanced Position Location Reporting System (EPLRS), which was initia lly fielded in 1972, was an altern ative to satellite-b ased position tracking of friendly ground forces. It did this by providing a secure IP -based data backbone th at networked digital position inform ation between each EPLRS ra dio operatin g across th e sam e network. Since th en its ro le h as shif ted f rom just a position tracking devi ce to e nabling lim ited types of general m obile wireless data netw orking for tactical comm anders. That is, it provided a platform for hosting applications other than position tracking. Unlike the SINCGARS, it does not provide in tegrated voice communica tions capa bilities, bu t the data throughput is significantly greater than that of the SINCGARS and is high enough to support externally connected voice over Internet Protocol (VoIP) technologies.

The EPLRS radio system ope rates within the UHF spectrum at between 420 and 450 MHz and is capab le of provid ing multiple devices simultaneous access to d ifferent types of data channels (different channels may use different MAC pr otocols), through its use of both Tim e Division Multiple Acce ss (T DMA) and Frequency Division M ultiple

Access (FDMA) resource sharing. The m aximum aggregate data throughput is between 525 and 1000 Kbps, depending on the version of EPLRS terminal being used. A regular PC can be connected   v ia an Ethernet port th at is built- in to th e EPL RS radio device, which is a much less restrictive in   terface th an the serial-to-data port PC connection required for a SINCGARS radio terminal.

The EPLRS radio device establishes its   data link s by crea ting a ser ies of permanent virtua l circuits (PVC) betw een different EPLRS devices, called *needlines*. A needline can be either many-to-many, few-to-many or one-to-one, and each EPLRS radio device can sim ultaneously communicate across 28 different needlines. Figure 5 shows a conceptual illustration of how EPLRS networ k resources are organi zed and divided into multiple needlines.
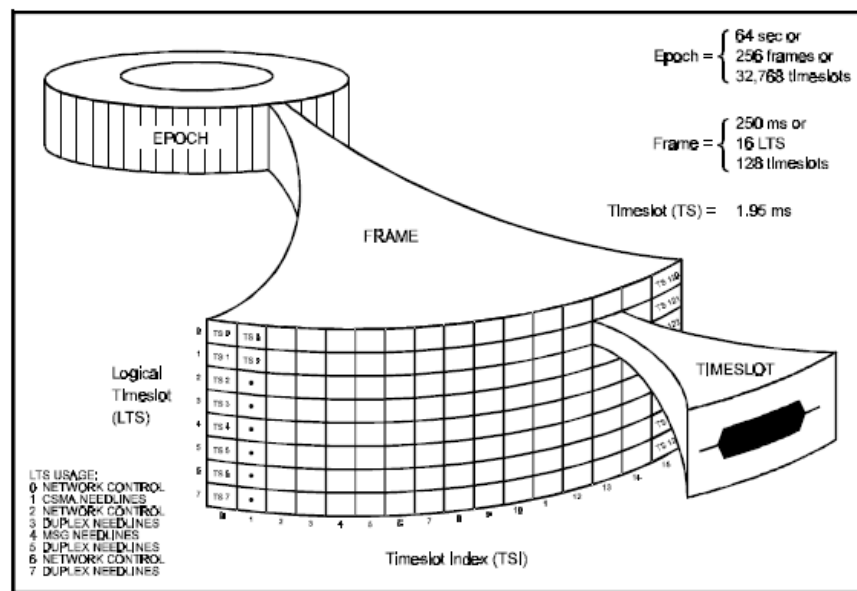
Figure 5.   EPLRS Epochs, Frames and Timeslots (From [12]).

The smallest division within a needline is the *time slot*. Each EPLRS radio device assigned to a particular need   line c an be assig ned one o r m ore tim e slots within th e needline. These tim eslots can be either 2 m s or 4ms in size, and ti me slot size m ust be consistent across the entire network (i.e., different needlines cannot operate with different time slot sizes). Tim   e slots are then grouped into   *frames*, which consists of 128 consecutive tim e slots. Groups of tim eslots within each fram e are combined in to eight

different *logical timeslots* (LTS) that span ac ross m ultiple f rames and can ea ch be assigned to different needlines. Frames are further group ed into *epochs*, which are 256 consecutive frames, which is the lar gest time division used in EPLRS. This m ulti-tiered method of organizing network resou rces allows the network manager greater flex ibility and control in allocating network resources to accommodate the n eeds of m any different types of users. However, this can also rest rict the am ount of resources available to any one needline, as once a resource is assigned to one needline it cannot be used by another. Each radio can support up to 32 separate need lines (4 of which are typically used for network control), which can be transmitted across any one of up to 8 frequency-separated channels.

Each EPLRS network is configured th rough the EPLRS Network Managem ent (ENM) suite, software that is hosted by a co mputer connected to an EPLRS radio. The ENM allows the network m anager to create ne edlines, assign network resources to these needlines and set the MAC protocols for each needline.

The EPLRS radio suppo rts many different MAC protocols. Since each needline operates on a separate lo gical channel from all th e other need lines, each needline can be assigned a different MAC protoc ol, according to the needs of the user. There are five main types of MAC pr otocols available to the EPLRS radio system : Carrier S ense Multiple Ac cess (CSMA), Multi S ource Group (MSG), High Data Rate (HDR) Duplex, Low Data Rate (LDR) Duplex and Dynamically Assigned PVC (DAP).

A CSMA needline allo ws m any-to-many trans mission capabilitie s ac ross the needline at data rates between 150 bps a nd 485.76 Kbps. CSMA needlines create one-time communication paths between two (or m ore) EPLRS radios, and transm issions sent via a CSMA needline are not acknowledged by the receiving EPLRS radios. E ven if there are multip le trans missions that m ust tr avel between th e same sets of nodes, since EPLRS nodes are typically highly mobile, these transm issions may not always be able to travel along the sam e path, so the path for each transm ission (i.e., the nodes that relay messages across m ulti-hop links) will be recalculated for each transm ission. Network resources are assigned to radios on-dem and, based on availability. W hile there is no guarantee of resource availability to any radio on the network, a m aximum hold tim e

value can b e set that p revents any one de vice from holding the needline resources for longer than the determ ined m aximum hold tim e. This ensures that one radio cannot prevent oth er radios f rom utilizing the n eedline, by perm anently captu ring the CSMA needline resources.

A CSMA needline can support a maxim um of 6 hops between originating and destination radios, but network m anagers can limit the allowed number of hops to 2 or 4, in order to reduce wasted bandwidth. Lo wering the maximum hop count reduces wasted bandwidth, because the EPLRS i mplementation of this type of needline requires each traffic originator to wait n-1 time slots between transmissions, where n is the m aximum hop limit, in order to ensure that the relay transmissions of tightly clustered nodes cannot interfere with the introd uction of new messages. All EPLRS radios do not act as a relay for all messages. Instead, the relay nodes invol ved in each transm ission path are chosen by a proprietary relay assignment algorithm that is processed by each receiving radio.

MSG needlines provide few-to-m any tran smission capabilities across an EPLRS network that guarantee s bandwidth f or up to 16 sim ultaneously transmitting radios, a t a data rate between 37.5 bps and 485.7 Kbps. MSG needlines create one-tim e communication paths between EPLRS radios , where traffic paths between nodes are recalculated for every transm ission, and tran smissions sen t via a MSG needline are not acknowledged by the receiving EPLRS radios. Specific time slots can be reserved within a MSG needline for specific radios, regardless of the radio's actual need for them , which is not poss ible us ing a CSMA needline. Al so, transmitting radio s must only wait f or a single tim e slot between its transmissions, re sulting in less wasted bandwidth than the CSMA needline.

LDR Duplex needlines provide one-to-one data links between two EPLRS radios at data rates between 20 bps and 16.2 Kbps, wh ich is very sim ilar to th e transm ission rates of the SINCGARS radio link. LDR needlines create two-way communication paths between two radio s, and each transmission acro ss this type of need line is acknowledged by the destination radio. Resources used for all LDR needlines on a network are reserved prior to the deploym ent of the network, and are allocated to specific LDR needlines on - demand, based on availability. If all of the LD R resources for a particular network are in

use, then a dditional L DR needlin e tr ansmissions will be delayed un til resou rces ar e released by other LDR Duplex needlines. Sim ilarly to M SG needlines, each relaying radio must only wait for a single time slot between its transmissions, in order to minimize wasted bandwidth.

HDR Duple x needlines are very sim ilar to LDR Duplex needline s. A ll of th e HDR resource ass ignment m ust occur pr ior to network de ployment, and will on ly be changed if an ENM adjusts th ese assignm ents during network deploym ent. The m ost significant differences are that the data rates for these needlines range from 600 bps and 242.9 Kbps, and network resources are reserved for each individual HDR needline. So, since all H DR needlines are not pulling from the sam e pool of ba ndwidth, there will always be network resources available for each HDR needline, eliminating the delays that could be experienced by LDR Duplex needline transmissions. The disadvantage of this is that while th ere are HDR needlines not activ ely sending data, the resources allocated for these needlines are being essentially wasted.

DAP needlines are simply either LDR or HDR Duplex needlines that are implemented on an on-dem and basis. Unlik e LDR and HDR needlines, they are not maintained throughout the operation of the network and are torn down once they are not needed.

While the currently deployed EPLRS ra dio does provide a fair amount of versatility for the configuration of relatively efficient data networks, its large size and the high power consum ption of the system prevent it from ever being a v iable candidate for providing highly mobile data connectivity to foot mobile troops.

C.   **COOPERATIVE DIVERSITY RADIO**

The prim ary purpose of this thesis is to com pare the network perform ance of existing ground-based tactical ra dio technologies to that of a specific radio device that uses emerging mobile wireless technologies, which was modeled in previous thesis work. Within this thesis, th is radio will be refe rred to as the Cooperative Diversity Radio (CDR). A very brief description of the CDR is given here, but more detailed descriptions can be found in [1].

The CDR is prim arily different from curre ntly available technologies in that it uses cooperative diversity, spatial slot reuse an d spatial pruning of data flow to perform multi-hop network flooding of a single wireless transmission significantly faster than any other known wireless technologies. It is de signed to provide both voice and two-way data communication services from the same handheld device. An external data device is still needed to create data for transmission ac ross a CDR network, that is, the device does not include any application hos ting capability. It does, ho wever, provide an 802.2 and 802.3 (Ethernet) interface to connect the dev ice to a wired network, in which case it serves as a bridge b etween the w ireless and wired dom ains, but as it does not host network protocols, it does not serve as a rout er, per se. The specific MAC protocol used for the CDR is not known, but it w as previously modeled using the slotted-Aloha MAC protocol, since this protocol was determined to provide the most meaningful observations regarding the performance of such a device.

In a CDR network, every rad io can act as a po tential relay for another radio's transmission. This does not m ean that all radios always relay all transm issions. A proprietary algorithm is used to ensure only the radios that are likely to be on the p ath between source and destination are used as relays during the creation of a two-way link between two nodes. The proprietary implementation transmits within the UHF frequency spectrum and has a m aximum hop count of 9 hops within a CDR multi-hop network, driven by the m aximum delay toleranc e of the m ulti-hop voice communications supported by the radios, a capability unavailable for either the EPLRS or SINCGARS.

Now that we have discussed the general characteristics of a variety of mobile wireless networking devices, we will now e xplain our m ethods for their ev aluation. Since we do not have the resources available to setup networks invol ving actual versions of each of these radios, we will ins tead an alyze an app roximation of their perform ance generated through the use of network simulation software.

The following chapte r discusse s ho w the ch aracteristics of these dev ices will b e translated into sof tware m odels, which will be used by softwa re n etwork s imulation programs to analyze an d com pare the perfor mance of each of these networks, und er a variety of network loads.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. JCSS IMPLEMENTATION

A.   JCSS NETWORK SIMULATION SOFTWARE

The Joint Comm unications Sim ulations Sy stem (JCSS) is a network s imulation software suite that has been adopted by the   Joint Chief of Staff J6 di   rectorate as the primary m ilitary ne twork m odeling and sim ulation tool f or the Department of Def ense. Formerly known as NETW ARS, it is m aintained by the Def ense Inform ation System s Agency (DISA), and provides the D epartment of Defense with a standardized tool for the analysis of the behavior and perform   ance capabilities of available defense communication networ ks. I ts main goa l is to a llow m ilitary co mmunication an d acquisition planners to identif y and quantify potential risks   and deficiencies that m ay exist with in network conf igurations prior   to their deploym ent and to validate any proposed hardware or configuration changes   made to existing system s. JCSS targets users ranging from lower level operational planners, who are attempting to quickly verify an equipm ent density list for a specific ope   ration, to higher leve   l analysts, who are attempting to estim ate network loa d lim its, ide ntify bottlen ecked links, or analy ze the performance and in teroperability of dif ferent software conf igurations ac ross wor ldwide networks.

JCSS can be generally divided into   two m ajor components: the network configuration interface and the capacity-p lanning interface. In the network configuration interface, th e user can choose from   a m enu of preconfigured communication nodes (or import custom nodes) and "drag-and-drop" them   into the software's workspace. The workspace can be a generic flat ar ea of various d imensions, or it can be made to simulate a very specific real   -life geographic location, incorpor   ating m ap infor mation, satellite imagery, and digital ter rain and e levation data, in order to in crease a s imulation's ability to reflect network performance within a specific geographic area.

Once all of the communi cation nodes are in place, each of them can be connected to each other with different types of comm unication links, as appropriate to the specific devices that define how each device will intera ct with the others. Also, each node has a

list of attributes that can be adjusted to   r eflect the ca pabilities and configurations available to the actual communications system being modeled.

Once the simulated network is f   ully c onfigured, the user can begin using the capacity-planning interface to start their analysis of the performance of various types and quantities of network tr affic. In o rder to accurately g enerate network traffic across the simulated network and   colle ct s tatistics related to th   is traf fic, JCSS operates   in conjunction with a commercially availab le OPNET Modeler ne twork sim ulation suite, licensed from OPNET Technology, Inc., which is described late r in this chap ter. Since this simulation engine contains many features that are not applicable to the configuration of military network models, JCSS attempts to streamline the OPNET Modeler simulation engine's in terface to make it m ore fam iliar to analys ts w ho are atte mpting to model military-specific communication networks.

As with any simulation model, the J CSS software suite does not provide an exact replication of radio performance within real-world scenarios. It does, however, provide a reasonably accurate fram e of reference for the com   parison of the advantages and disadvantages of em ploying various types of networked devices under m any diffe rent network conditions.

1.   OPNET Modeler Network Simulation Suite

The OPNET Modeler network simulati   on suite was designed to model the performance of m any different types of   commercial data and voice communication devices and to provide the user   with tools to easily analy ze the perform ance of these devices under a wide variety of configura   tions. OPNET Modeler a lso allows f or the creation and analysis of custom ized communication device models a nd model processes, which means that the user is not limited to the use of the preconfigur ed models that come packaged with the software. Since all of   the JCSS network sim ulation capabilitie s are derived through its use of OP   NET Modeler device node models   and its discrete event simulation kernel, it is im   portant to   understand how the OPNET Modeler software functions, and how it is able to   model specific types of tactical radio nodes. The rest of this chapter includes a summary of the more specific descriptions of the functionality and

capabilities of OPNET Modeler compiled in [5]. All of the simulations performed in this thesis were run using OPNET Modeler version 14.5.

2. Node Models

Since the o bjective of most m odeling e fforts is to observe the behavior and measure the overall perfor mance of networks consisting of m any node s, it is critically important that the m odel of each node in cluded in the network is sufficiently representative of the actual device being m odeled, as well as an appropriate m odeling of the expected traffic types and volumes. It is important for the OPNET Modeler user to be familiar with the general node m odel design m ethods use d to create the m odels of the devices included in their simulation.

A node m odel is a software representati on of an actual netw ork device. Each node m odel contains its own internal proc esses that operate independently of the processes contained by other node models within the sam e network. E ach node m odel can execute multiple processes and can contain multiple types of interfaces between other nodes. There are different characteristic va riables for each node m odel that lim it its behavior to actions that mimic those performed by the device being m odeled. A model's performance characteris tics can be adjusted by altering the availab le configuratio n settings for each model. Each model configuration setting is designed to reflect the types of setting s availab le on the actu al device be ing m odeled, but m any m odels inc lude settings that are not found on the actual device, in order to m ake it easier for the user to quickly configure a sim ulation where specific co nfiguration settings are not im portant to the analysis being performed.

The actual functionality of each node m odel is defined by a finite-state-m achine set of process m odels that dete rmine whic h of its processes are called at different simulation tim es and in response to different received signals from ot her nodes. Each state transition in the various process m odels is defined by blocks of C or C++ code that control the behavior of each proces s, and the order in which each state is reached as the simulation progresses.

31

Each proces s m odel can be altered at the code level, in order to give the user complete control over the functionality of customized communication nodes. This ability to allow de tailed cu stomization of vari ous types of node m odels gives an OPNET Modeler user the ability to simulate the performance of nodes that do not exist in real life, or for which there is no ready-made model provided.

3.   Discrete Event Simulation Kernel

The discrete event sim ulation kern el is the "brains" of each network simulation. It orchestrates the generation and processing of a ll events that occur during a sim ulation. While there are thirteen speci fic types of events recognize d by the sim ulation kernel, the definitions of each specific event is well beyo nd the scop e of this particular th esis. In general, an event is one of two types of actions: It is either an instance of one node sending network traffic to another node, or an instance of a process within a single node communicating with a different process of th e sam e node, such as the encapsulation of one protocol data unit into another. When any node requires an action to be performed, it sends an interrupt to the discrete event simulation kernel, which is queued and processed according to the needs of all other nodes with in the same network. Since only one event can have access to th e kernel resou rces at a tim e, it is the discr ete e vent sim ulation kernel's job to ensure that the resulting behavior of any portion of the network simulation is m inimally affected by the order in which each even t is process ed. In ord er to accomplish this, th e dis crete event sim ulation kernel m ust be able to process ev ents serially in a m anner that makes it appear as though they were processed in parallel. This is because each simulation will like ly be modeling multiple communication devices tha t would norm ally be functioning sim ultaneously in a non-sim ulated environm ent. However, by dividing a continuous tim eline into sufficiently sm all di screte intervals, each interval can be established such that only one event occurs during that interval.

In order to achieve effective event processing, the discrete event simulation kernel uses an event list to manage each event. Instead of using a simple FIFO queuing method, where each generated event is queued based on when it was processed by the kernel, each kernel event has a simulation-time timestamp and is placed in a proprietary data structure

(no specifics of the exact f unctionality of this data structu re were give n in the OPNET Modeler do cumentation) based on each even t's sim ulation-time tim estamp. So, i f an event is generated with a simulation-time that is earlier than that of the event curren tly at the head of the data stru cture, the new event will be sche duled for processing before all other currently scheduled events. This essen tially makes us e of a type of priority queue data structure.

4.   Link Models

OPNET Modeler has th e ability to model many different ty pes of physical layer links between networked nodes. The included li nk models range from Ethernet and fiber optic cab les to sim ple single ch annel ra dio wave transm issions and com plicated frequency hopping transm issions. Since the only physical layer link used for sim ulations in this thesis is wireless radio wave transmissions, this section will focus on how OPNET Modeler represents radio wave transmissions in its software.

Each link simulated in OPNET Modeler is represented by a series of pipeline stages th at s imulate the physical effects of the transm ission m edium on the transm itted signal. Pipeline s tages are implemented as procedures written in C or C ++ programming languages. Each procedure typically takes a   simulation-packet data type as their only argument, and returns a sim   ulation-packet da ta type to the wireless   receiver of a networked node.

For wired links, the pip eline effect on each tran smission can be computed once at the beginning of the si mulation and the sam e pipeline can be used throughout the entire simulation, as the characteristics of a wired   transmission m edium rem ain static. Since there are so m any variab les that can have a significant effect on wireless transm issions, wireless lin ks m ust be evaluated d ynamically at each s imulated pack et broadcast. At each signal broadcast, a series of virtual links are created between the transm itting node and any wireless receiv ers with in range of the transm ission. Once each virtual link is established, a copy of the transm itted packet is created fo r each link and a pipeline analysis is p erformed on each individual copy of the transmitted packet. Each s tage of the pipe line analys is ta kes into con sideration a different environm ental or signal f actor

33

that would have a significant effect on an actual radio wave transmission. Since no actual radio waves are trans mitted, the analys is results are found m athematically, u sing characteristics of each simulated tran smission (i.e., power le vel of the transm itted signal and physical dis tance b etween th e transm itter and receiver) and formulas involving known physical characteristic s of the real world (i.e., the propagation delay d of a signal travelling distance r will be $d = r/C$, where C is the spe ed of light). For the Radio transceiver Pipeline, there are fourteen stages, each of which is briefly described below:

a.   Receiver Group

This stage is executed one tim e at the beginning of the si mulation. The purpose of this s tage is to de termine which nodes are likely to communicate with each other, based on link type and relative position, in order to prevent the rem aining pipeline stages from unnecessarily analyzing the effects of nodes that are of a different type or are currently too far away to have any effect on the link being analyzed. This stage has no influence on the perform ance or behavior of the network being sim ulated, and is only included to m inimized the am ount of total tim e it take for the sim ulation to run, by eliminating unnecessary calculations.

b.   Transmission Delay

Based on th e packet size and trans mission rate of the tran smitting node model, this stage calculates the am ount of total tim e that passe s from when the node begins to transm it its signal to when the node com pletes its transm ission. This is information will b e us ed to c alculate the f inal res ults of later p ipeline stag es a nd is executed once per transmission.

c.   Link Closure

Since the R eceiver Gro up stage an alysis is only perform ed at the very beginning of the sim ulation, this stage accoun ts for potential changes to the topo logy of the wireless nodes in the network that have occurred since the sim ulation began, and adjusts the list of nodes to be considered for si gnal interference processing. This stage is

performed once per receiving channel and has no influence on the perform ance or behavior of the network being simulated. It is only included to m inimize the amount of total time it takes for the simulation to run, by eliminating unnecessary calculations.

d. Channel Match

This stage s imply compares the cha nnel frequency settings of both nodes on each virtual link. If the frequencies of bot h nodes on a particular virtual link match or are close en ough to potentially in terfere with each other, th en the tran smission will b e forwarded to the next stage of the pipeline anal ysis. If they do not match, then the virtual link between the two nodes is no longer consider ed for further pipeline analysis of the current transmission.

e. Transmitter Antenna Gain

During this stage, the in tensity of the transmitter's signal in the dire ction of the receiving node is calculated and used later in the pipeline an alysis, in order to determine if the transmission's strength is great enough to reach the receiving node. This variable is of special significance to nodes transmitting with directional antennas.

f. Propagation Delay

This stage c alculates th e sim ulation-time at which both the leading an d trailing edg e of the tran smission actually reach the receiv ing node. This inform ation is used later in the pipeline analysis to determ ine if any other signals ar rive at the receiving node during the reception of the transmission being analyzed.

g. Receiver Antenna Gain

During th is stage, any increase in in tensity of the signal received by the receiving no de from the use of directional an tennas is calculated a nd used later in the pipeline analysis.

h.   *Received Power*

This stage calculates the actual pow er of the signal received based on the transmission power, antenna gains and node di stance, which were pr eviously calculated by earlier s tages of the analysis. This inform ation is ultimately us ed to determ ine if the transmission's strength is gr eat enough to overcom e any i nterference from any other transmissions received at the same simulation time.

i.   *Interference Noise*

This stage calculates the noise created by other transmissions, based on the power of each interfering signal and the duration of each interfering signal.

j.   *Background Noise*

This stage calculates the noise create d by other sources of electrom agnetic radiation that have been introduced into a si mulation. These values are based on the type of background noise and its proximity to the receiving node's antenna.

k.   *Signal-To-Noise Ratio*

This stage calcula tes the signal-to-no ise ra tio f or eac h part of the transmission, using the received po wer, inte rference noise and backgrou nd noise values determined in earlier pipeline stages.

l.   *Bit Error Rate*

This stage determines the expected bit error rate of the transmission based on the s ignal-to-noise ratio ca lculated a cross the en tire transm itted f rame. Greate r amounts of noise will produce a higher probability of erroneous bits.

m.   ***Error Allocation***

It is at this stage that actual errors are introduced into different parts of the transmitted frame, based on the bit error r ate probability values determ ined for different sections of the transmission.

n.   ***Error Correction***

No error correction algo rithms are actually performed during this stage of analysis. In stead, th is s tage sim ply decide s whether or not to discard the transm ission based on calculations that are perform   ed us ing probability distributions based on the specific error correction mechanisms being used in the network and the total num ber and locations of the introduced bit errors.

5.   **Application Profiles**

In order to consistently sim ulate many di fferent types of netw ork traffic across a network with m any different nodes, OPNET M odeler allows its users to use application profiles that mimic various combinations of network traffic that may be produced by each node. This m akes confi guring m ultiple instance s of the sam e type of user quicker and more consistent. If adjustm ents need to be   made to an ap plication pr ofile prio r to th e execution of a simulation, once changes are made to the profile they will automatically be reflected on all nodes a ssigned to that profile. This is   especially useful when running different variations of the same general simulation scenarios.

While som e preconfigured application pr ofiles that sim ulate common types of network activity (internet br owsing, email, ftp, video confer encing, etc.) are provided, it is also possible to create and configure cust   om application s that gener ate the spec ific types of traffic across the network. Differe   nt application profiles   can be assigned to different nodes, and a single node can be assi gned multiple profiles. These application profiles can also control the frequency and destination of defined traffic flows.

Since the mode and te mpo of inf ormation f low in m ilitary communications can vary significantly from that of a typical business office network, the custom application options were best suited to m odeling data tr affic of tactical data networks in our simulations.

6. Data Collection

OPNET Modeler allows the use r to collec t data on any kind of event generated during the sim ulation. Statistics can be collect ed for the network as a whole, or for any single link, node, or application operating within the simulated network. The user simply selects the types of data to be collected pr ior to running the simulation, and then after the simulation is com plete, the co llected data can either be displayed v ia an inclu ded graphical interface, or exported to separate programs for analysis.

B. JCSS SINCGARS MODEL

In our network sim ulations, we will us e the SI NCGARS node m odel included with the JC SS version 8.0. W e have m ade no a lterations to this m odel and, in order to establish a basis for comparison to the CDR node, will attempt to introduce the same type of network traffic using the SINCGARS model as the network's physical layer transmission device. This section briefly explains how the SINCGARS r adio is modeled in JCSS.

1. Node Model Logic

In order to accura tely model the func tionality of the SINCGARS radio, JCSS software provides a dev ice model that attem pts to replicate the logic b ehind the flow of data through a SINCGARS radio term inal. As depicted in Figure 6, the internal organization of the node m odel divides all of the separate functions into individual process models (the gray squares), which are able to communicate with other pro cesses, as indicated by the red and blue arrows.

Figure 6.   SINCGARS Node Model

The Application process model (*application)* represents the applications available to the SINCGARS radio, which consist solely of analog sound wave input and output via the radio handset. The Transport-to-Application process model (*tpal*), which is present in most OPNET device models, provides an interface between the application and trans port protocols available to each device m odel. This s imply allows each application m odel to be reused by m ultiple types of devices. The Transport P rotocol pro cess m odel (*se*) represents the only transport pr otocol available to this m odel, and the Packet Forwarding process model (*fwd*) merely determines the proper forwarding direction for each packet it encounters (analog voi ce is sent to the   *se* model and analog data is sent to the *sincgars_inc_mac* process). The SINCGARS Da   ta Inte   rface   process model (*sincgars_inc_mac*) represents the interface between the radio terminal and the externally connected Internet Controller (INC).   The Media Access Control process m   odel (*mac*) simply models the interface between the radio and its antenna.

2. Node Model Configuration

For data communications, we will also incorporate the SINCGARS INC interface model into each node. The INC functions as a basic IP router and allows a normal computer to connect to the SINCGARS radio via an Ethernet port. OPNET Modeler provides SINCGARS INC interface model (*sincgars_inc_adv*), shown in Figure 7, that provides the logic behind the data routing and MAC protocol capabilities of the SINCGARS INC module.
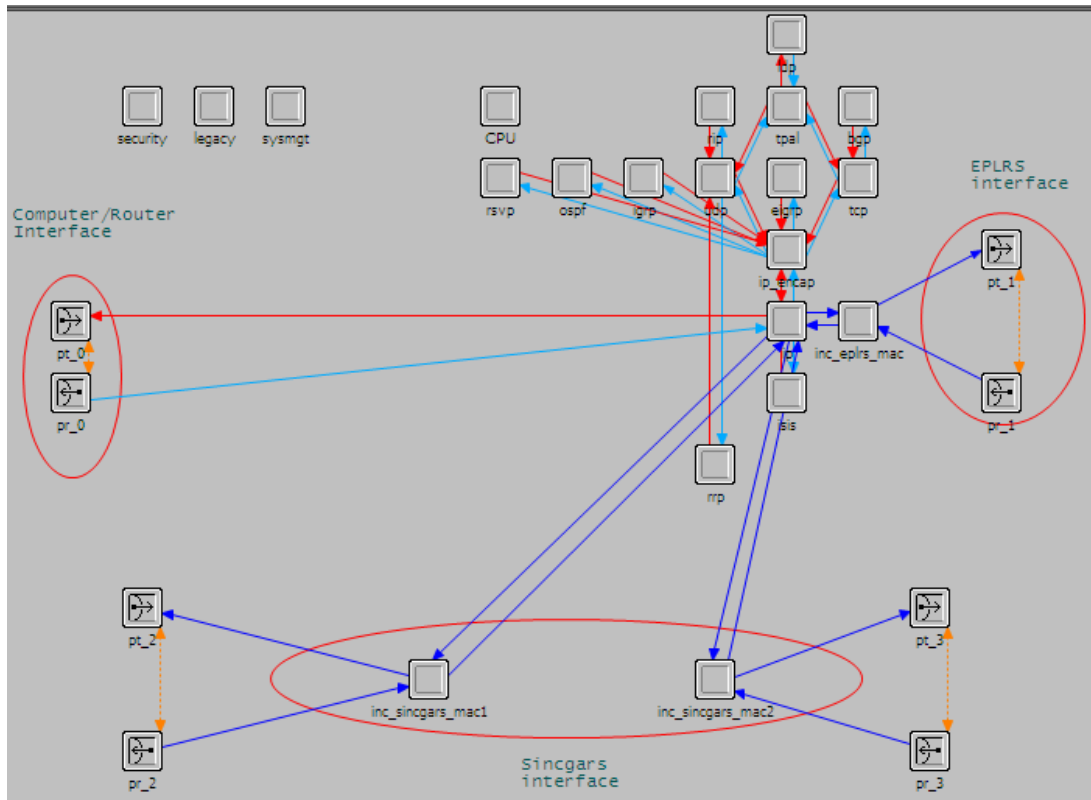
Figure 7.   SINCGARS Internet Controller Model

Notice that there is no *application* process module included in the SINCGARS INC interface model, like there is in the SINCGARS radio terminal model. This is because there are no voice communication functionalities to model the INC, as all voice communications are not handled by the INC. Additionally, any applications that would be producing data traffic for transmission through the INC would be hosted on an externally connected data device. Since the only task performed by the INC is deciding

how to route various types of data transmissions, the application process is replaced by a Label Distribution Protocol process model (*ldp*), which builds and maintains a database of its peer nodes for transmission relaying purposes. The Transport-to-Application process model (*tpal*), simply acts as an interface between the ldp and udp and tcp processes, so the same ldp process can be reused by other device models. Both the Transmission Control Protocol (*tcp*) and User Datagram Protocol (*udp*) process models are included, since the INC supports both types of transmissions. The IP encapsulation process model (*ip_encap*) performs the packet encapsulation functionality for the Internet Protocol process model (*ip*), which focuses on the forwarding required to run the IP protocol. The EPLRS MAC (*inc_eplrs_mac*) and SINCGARS (*inc_sincgars_mac1/2*) process models control both incoming and outgoing packets' access to the INC Ethernet port, both SINCGARS data ports and the EPLRS data port.

C.   JCSS EPLRS MODEL

In our network simulations, we will use the EPLRS node model included with the JCSS version 8.0. We have made no alterations to this model and have decided to use CSMA needlines as the MAC protocol, since it is the only many-to-many capable needline currently supported by OPNET Modeler. This section briefly explains how the EPLRS radio is modeled in JCSS.

1.   Node Model Logic

In order to accurately model the functionality of the EPLRS radio, JCSS software provides a device model that attempts to replicate the logic behind the flow of data through an EPLRS radio terminal. As depicted in Figure 8, the internal organization of the node model divides all of the separate functions into individual process models (the gray squares), which are able to communicate with other processes, as indicated by the red and blue arrows.
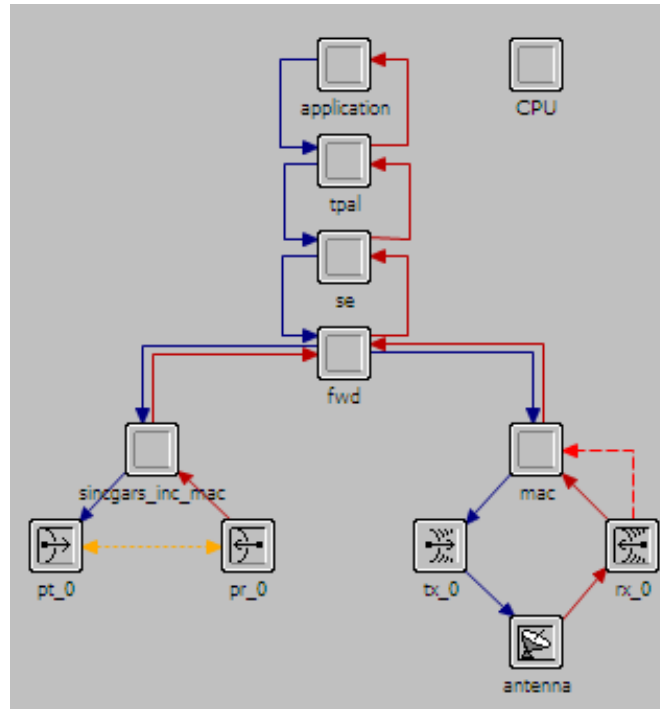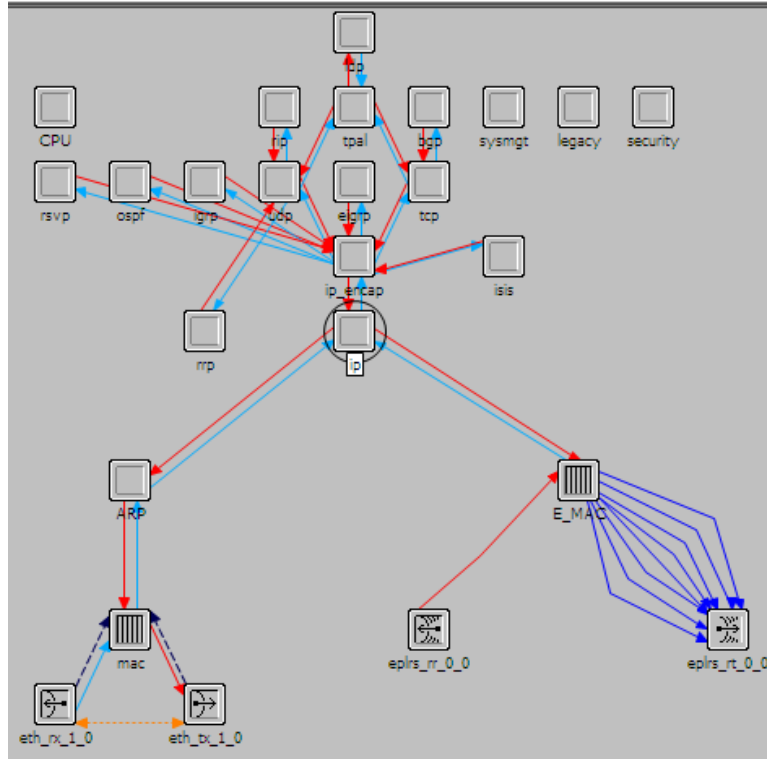
Figure 8.   EPLRS Node Model

Similar to the SINCGARS INC m odel, ther e is no *application* process module included in the EPLRS node m odel. This is because there are no voice comm unication functionalities to m odel f or this ra dio, a nd any data applicati on requiring use of the EPLRS network will be hosted on an externally connected computer. Since the only task performed by the EPLRS is deciding how to   route various types of data transm issions, the application process is replaced b y a La bel Distribution P rotocol process m odel (*ldp*), which simply builds and maintains a database of its peer nodes for transmission relaying purposes. The Transport-to-A pplication process model (*tpal*), simply acts as an interface between the ldp and udp and tcp processes, so   the sam e ldp process can be reused by other device m odels. Both the Transmission Control Protocol (*tcp*) and User Datagram Protocol (*udp*) process m odels are included, si   nce the ELRS supports both types of transmissions. The IP encapsulatio   n process model (*ip_encap*) perf orms the packet encapsulation functionality for the Internet Protocol process model (*ip*), which focuses on the forwarding required to run the IP   protocol. The EPLR   S MAC process model (*E_MAC*) simply controls each tran   smission event's access to the physical transm   itter

42

process m odel, while accepting incom ing tr ansmissions from the physical receiver process m odel, in a manner th at m imics th e genera l f unctionality of the prop rietary EPLRS MAC protocols that route traffic in actual EPLRS networks. The Address Resolution Protocol process m odel (*ARP*) m aintains a queue of outbound packets that still need MAC addresses to be delivered and generates an ARP request and response for these p ackets. The M AC process m odel (*mac*) controls both incom ing and outgoing packets' access to both EPLRS Ethernet ports.

2. Node Model Configuration

The EPLRS radio only handles the rou ting and MAC protocol enforcem ent for data tran smissions acro ss the EPLRS network, so an extern al network interface dev ice needs to be connected to an EPLRS in ord er to crea te app lication d ata. As a resu lt, a similar INC interface m odel is utilized for use with the co nnection of data p rocessing devices to an EPLRS device model.

D. JCSS TACTICAL APPLICATION MODELS

In this s ection, we will explain th e various data applicatio n sets that could be expected to be em ployed across different type s of tactical data networks, and how these applications are represented in our JCSS network sim ulations. For consistency purposes, we will attem pt to recreate the tactic al a pplications an d prof iles used in [1]. A description of each application m odel and d ifferent application profiles are prov ided in the following sections.

1. Application Model Definitions

The specifications for an application th at allows a network node to introduce traffic into its network are de fined as application m odels. The m odels utilized in our simulations are summarized in Table 2, and explained in more detail below:

Application	Service	Msg Size (Distr)	Destination	Interarrival (Distr)	Success
Unicast to gateway	UDP	50 B (const)	gateway	1 min (const)	3 min
Unicast with ACK	UDP	20-160 B (uni)	unicast	10 min (exp)	10 sec
Constant Multicast	UDP	1066 B (const)	multicast	66.6 msec	90% 3 sec
Bursty Multicast	UDP	67-333 x 40 B (const) @ 33.3/sec	multicast	30 sec (exp)	90% 0.25 sec
IRC from client	TCP	20-512 B (exp)	gateway	10 min (exp)	10 sec
IRC from server	TCP	20-512 B (exp)	client	5 sec (exp)	10 sec
TCP push	TCP	500 B – 1 MB (exp)	gateway	15 min (exp)	2 min
TCP pull	TCP	500 B – 1 MB (exp)	client	15 min (exp)	2 min

Table 2.   Summary of Modeled Application Set (From [1])

a.   Unicast with ACK: Short Message

This custom application m odel is de signed to m imic sm all, irregularly transmitted, text-ba sed m essages, such as send ing a single text m essage or digital call-for-fire request. Each source node will randomly choose one of its designated destination nodes and send that node a single TCP transmission, ranging in size from 20 bytes to 160 bytes. This traffic will be introduced appr oximately one time every 1200 simulation-time seconds, with an exponential distribution.

b.   Unicast to Gateway: Position Update

This custom application m odel is   designed to m imic sm all, regularly transmitted data m essages from each client node to the network's gateway node, s imilar to position update transm issions. Any node running this application will send a 50 byte UDP segment to the network's gateway node once every minute.

c.   Constant Multicast: Video

This application m odel takes advantag e of the preconfigured application models provided with OPNET Modeler. It allows a network node to pull video-only data from the network gateway node. Because of limitations of the MAC protocol used by the CDR node, the video fram e size was reduced to   500 bytes at a rate of 2 fra   mes per

44

second. Although these traffic characteristics are not representative of norm al streaming media, we will keep these sam e f rame size and rate se tting f or our sim ulations f or accurate comparison purposes to the simulations performed in [1].

d.   IRC

This is a custom application m odel that is designed to m imic the type of traffic load introduced to a network by intern   et relay chat (IRC) applications. Traffic originates from a network node and is sent to the network's gateway node, which initiates a series of m   essage exchanges that o   ccur between the two nodes. There are approximately 60 send/receive ex changes that occur each time an IRC event tak es place, and each no de's response is delayed for an av erage of 5 seconds, in order to sim ulate message-typing response times.

e.   TCP Pull: HTTP

This is a custom   applica tion m odel that m imics the type of   traf fic introduced by various network nodes requesti ng HTTP downloads across the network. This application begins with a fixed-size HTTP request of 400 bytes from a network node to the ne twork's ga teway with the tim e betw een requests varying exponentially with a mean delay of 900 seconds. Each requested   page size varies uniform ly between 500 bytes and 1 MB.

f.   TCP Push: Email

This is a custom application m odel that roughly mimics the type of traffi c that m ight be introduced by various nodes   uploading em ail m essages to the network gateway for delivery. Each email message varies uniformly between 500 bytes and 1 MB and is uploaded at tim e intervals that vary   exponentially with a m ean of 900 seconds. This m ay be an unrea listic rate of typica l tactical em ail u sage, as we would expect numerous emails to be sent within only a few minutes of each other, w hile there is a lull in operations, then have much longer periods of no emails, as the tactical commanders are occupied with other operational tasks. However, for the purposes of a three-hour

45

simulation, it provides a reasona ble reflection of how e mail-sized traffic m ay affect the overall network perform ance in the presence of other running applications. Once the upload is com plete, the server acknowledges the upload with a 500-byte m essage that ends the application event.

2. Application Profile Definitions

Every node within a simulation network will introduce qu antities and types of traffic onto its network according to the appli cations models assigned to it. Since most node users will typically use m ore than one type of appl ication, applications for our simulations have been grouped into application profiles that correspond to the type of user at each node.

In addition to grouping applications, since it is unrealistic for each node to begin transmitting traf fic at precis ely th e sam e time (i.e., at the very beginning of the simulation), our application profiles allow a dditional configuration options that control the simulation start and stop times for executi ng the application events for each type of user and the frequency that these ev ents are executed. In order to be consistent with the simulations run in [1], we have set all of our application profiles to random ly begin the execution o f their application events so mewhere between 60 a nd 600 sim ulation-time seconds after the beginning of the simulation.

a. Tactical Commander

This applic ation p rofile m odels the types of traf fic in troduced to the network by platoon and company commanders. Due to configuration limitations inherent to OPNET Modeler 's implementation of the ap plication profile, the needs of the tactical commander node had to be divided into two sepa rate custom profiles. This is because some of the application s will b e run constantly through the entire s imulation, and other applications will only run at randomly generated time periods during the simulation. The first profile is assigned the IRC applicati on model, which will be runnin g throughout the entire simulation. The second profile will be assigned th e Position Up date, TCP Push:

Email and TCP Pull: HTTP application m odels. This prof ile has so m any application s because it is typically o nly the tactical co mmanders who perform these kinds of events frequently and simultaneously.

b. Fire Support

This applic ation p rofile m odels the types   of traf fic in troduced to the network by a forward observer for fire support. It has the exact the same requirements as the Tactical Comm ander profile, bu t because th ey are two very different jobs, a s eparate profile was created, in o rder to allo w scenario adjustments to the behavior of one type of node without affecting the behavior of the other.

c. JTAC

This applic ation p rofile m odels the types   of traf fic in troduced to the network by a JTAC (a special t ype of forward observer). Fo r our simulations it will only be assigned the video ap plication model; however, in some scenarios the JTAC will have similar requirements to those of the Fire Support profile.

d. Gateway

For our simulation s, the network gateway node will not actually run an   y applications itself, so its application profile will not actually be ass igned any application models. This node will, however, be the sour   ce or destination of traffic generated by many of the non-gateway nodes, such as the   Unicast to Gateway, TCP Push: Em ail, and TCP Pull: HTTP application profiles.

e. Position Update

This applica tion prof ile will m imic the type of traf fic intro duced to th e network by a node reporting its position to the gateway node. Each network node will be assigned to this p rofile, and it will produce traf fic concurren tly with other app lications running at the sam e node. It was kept sepa   rate from othe r profiles in order to create baseline simulations that have position reporting as the only traffic intro duced across the network.

f. Short Message

This profile will represent nodes that are sending sim ple text m essages across the network. It was kept separate from other profile, in order to create additional baseline simulations that have sm all text m essages as the only traf fic introduced acr oss the network.

Now that we have discussed how our network simulation software works, its capabilities and lim itations, and how actua l communication devices and traffic loads can be trans lated in to software m odels, we will now begin our analysis of each radio network's performance under different simulated network conditions.

The following chapter will discuss the network performance data collected from software simulations involving both SINCGARS and EPLRS net works, attempt to explain each network's perform ance and com pare the r esults to s imilar sim ulations collected in [1], involving CDR networks.

V. EXPERIMENTAL SETUP AND RESULTS

A. EXPERIMENTAL SETUP

In th is ch apter, we will com pare the ne twork sim ulation resu lts of scenar ios involving SINCGARS and EPLR S tactical radios to thos e involving the CDR, as presented in [1]. Once the r esults a re p resented, we will disc uss the va rying performances of each tactical radio model in networks of sim ilar size and under sim ilar traffic loads. All of the tactical radio node models used in these scenarios are unaltered and reflect the general performance characteristics of actual tactical radios.

For each radio, we will run sim ulations configured for both a platoon-sized network (6 nodes) and a com pany-sized netw ork (20 nodes). Each network will be populated with five levels of gradually increa sing traffic loads, each of which reflect the estimated traffic loads of various com binations of tactical data applications. T he applications included in each of the five load levels are sho wn in Table 3, with the load level descriptors listed in the leftmost column and the available application profiles listed in the top row. The application p rofiles r unning at each load level are indicated with marks placed along each load level's row, under each application profile included at that level.

	Tactical Commander	Fire Support	JTAC	Position Update	Short Message
Position Update Only				X	
Short Message Only					X
Commanders and Position	X			X	X
Currently Deployed Applications			X	X	X
All	X	X	X	X	X

Table 3.   Application Profile Sets For Network Simulations (From [1]).

For the simulation s inv olving SINCGARS networks, each node consists of a SINCGARS radio term inal m odel that prov ides the physical layer component of each node. This SINCGARS radio te rminal connects to generic Et hernet workstation m odel, via a S INCGARS Internet Contro ller m odel, which provides an appropriate interface between the two devices. All network traffi c is generated and re ceived by the generic Ethernet workstation at each node, with the ex ception of the Gateway node, where a generic Ethernet server model is used instead. E ach SINCGARS radio term inal is set to the m aximum 16 Kbps through put and all wired connections between m odels is 100BaseT or higher. All SINCGARS nodes acc ess the transm ission medium as soon as they have m essages to transm it, esse ntially imple menting a regular ALOHA MAC protocol across the network, and the only type of quality control im plemented across this network is the us e of TCP by select appli cations. Othe rwise, if a m essage's initia l transmission experiences a collision, it is never retransmitted by the node.

In each EPLRS network sim ulation, each no de consists of an EPLRS radio terminal model that provides the physical layer component for each nod e. It connects to a generic Ethernet workstation m odel thr ough an EPLRS r outer m odel interface. All network traffic is generated and received by the Ethernet workstations, with the exception of the Gateway node, where a ge neric Ethernet server m odel is used instead. All nodes are members of a CSMA needline assigned th e maximum of 4 usable LTSs, and is set to use waveform 4, which allows a m aximum throughput of 311 Kbps (the waveform with the highest throughput of all the available JCSS EPLRS model waveforms). Each node is set to allow a maximum of 6 hops, which, given the nature of the EPLRS CSMA needline implementation, reduces the effective throughp ut utilization to 1/6 of the m aximum needline throughput, or 51.83 Kbps for our scenario.

Unlike the SINCGARS, each EPLRS node will first check to see if th ere are an y other m essages being transm itted bef ore b eginning to send th eir own m essage, implementing a CSMA/CA MAC protocol. If the node senses another transm ission, it will queu e its m essage and check the m edium again late r (after a rand omly gener ated delay). Eac h tim e it se nses tha t th e m edium is busy, it w ill choo se a n increm entally longer back-off delay, until it sens es no other tr ansmissions, at which tim e it will start

sending its own message. Since we could not find a maximum needline hold time setting for the JCSS EPLRS node m odel, we will assume that each node in each of our simulations controls the transm ission m edium (potentially indef initely) until it is d one transmitting.

For both sets of simulations, each node will remain stationary, and each node will be within transm ission rage of every other node. W hile the spe cific scena rio b eing simulated in this thesis does not require the transm ission of more than one hop, it assumes that the nodes that support m ulti-hop cap abilities are configu red to allow the maximum a llowed hops, in preparation for fo llow-on m obile operations, where nodes may not be within one hop of each other. Sin ce the EPL RS nodes do not dynam ically adjust the hop count settings based on perceived network t opology, it is fair to assum e that even w hen each no de is with in one hop from all o ther nodes, its p erformance will still be lim ited by the network's m aximum hop count settings. Also, different needline configurations handle multi-hop delivery differently, and m ay pr oduce differen t performance ratings. F or com parison purposes , we attem pted to choo se the typ e of needline th at most closely resem bles the conf iguration settings of the CDR analyzed in [1], in order to produce results that dem onstrate the im pact of the general differences between each device. The performance of different needlines and more dynamic network scenarios, where the relative distan ces betw een each node is constan tly increasing and decreasing are left for future research.

The following are explanations of each traffic load level:

### 1.	Position Update Only

This applic ation traf fic load level consists o f m essages that are r egularly transmitted once every minute, and represent position location messages being sent by all nodes attached to the network to the network's gateway node. This scenario is included to verify that correct connectivity confi gurations exist between each node in the simulation. It also provides a baseline fo r perform ance c omparisons to other radios operating under the sam e load level and to simulations of the sam e network operating under more demanding load levels.

2. Short Message Only

This application traffic load level consists of slightly larger text messages that are transmitted at exponentially vary ing tim es across the network. This application represents text m essages being sent between two nodes attached to the network. This load level is included to show each networ ks ability to ha ndle simple text m essaging traffic that is currently in use by existing tactical radio networks.

3. Commanders and Position

This applic ation traf fic load level includes a ll of the modeled tac tical data applications except for stream ing video. Th is level is included to dem onstrate each network's ability to function when supportin g all but the m ost bandwidth intensive application.

4. Currently Deployed Applications

This traffic load level is meant to mode l each ra dio's ability to handle all of the tactical data applications currently in use by tactical mobile nodes. Since m any of these applications are accessed at a single node throu gh separate networked radio devices, if a network composed of a single t ype of radio device is shown to be able to support all of these applications at on ce, then it w ould be reasonable to think that it would be possible to streamline each node's equipment load to only one radio device.

5. All

This traffic load lev el includes som e applic ations that are not currently available to users operating at the lowest lev els of tactical command (i.e., E-m ail and IRC), and it serves as an ultim ate com parison scenario for a particular radio network's ab ility to support an ideal application environment for users at the platoon and company levels.

B.   PLATOON SIMULATIONS

Our platoon-sized network sim   ulations consist of six radios: one platoon commander, three squad leaders, one m   ortar platoon, and one ga teway node. Figure 9 depicts the location of each radio model within the simulated network.

Figure 9.   Platoon Network Layout

Each node attached to the network is li mited to tran smitting the types of traffic allowed by the application profile associat   ed with that particular node during   each scenario. So, depending on the scenario so   me nodes m ay introduce different types and quantities of network traffic th an the other nodes. The appli cations associated with each node attempt to mimic the types of traffic that would be reasonably expected from the job assigned to each node. For exam ple, a squad leader is only allowed to use the position update and short m essage applications, the   mortar platoon can only use the position update, short m essage and fire support appli cations and the platoon comm ander can use all application profiles. The gateway node does not initiate the use of any applications. It only acts as a source for streaming video, a recipient of position report data and source of TCP application traffic, for nodes sending TCP traffic that is routed through the gateway.

1.   Position Update Only

All three networks were able to succe   ssfully support this   network simulation scenario. The SINCGARS and EPLRS ne   tworks each achieved a 100% m   essage delivery success rate, and the results presen   ted in [1] show that the CDR network achieved a 99.6% m essage delivery success ra te, missing only four m essages during the 15 hours of total simulation time.

The fact that the CDR did not achieve a   100% success rate is a little surprising. Since all ap plication tra ffic being introduced into the Pos   ition Update Only sce   nario enters the network at a constant rate (each node transm   itting the sa me message in a 60 second cycle), and all nodes ar e stationary, if the collisions were caused by two nodes attempting to introdu ce new traf fic at the same tim   e, we would expe   ct to s ee th ese interferences occurring much more regularly (once per 60 s econd cycle, or 180 collisions per 3 hour simulation), producing more than a total of only four missed messages.

Additionally, if the collis   ions w ere caus ed by interf   ering m essage relay transmissions from m ultiple CDR nodes, we w   ould expect this type of interference to occur at a constant rate, as well. Since there were no other generic sources of environmental noise introduced into this scenario, the only source of signal noise that can affect each simulated transmission are transmissions from other nodes. With such a high number of different "simultane ous" CDR relay events being processed in serial by the discrete event kernel, it is possible, but unlikely, that th ese transmission collisions could be attribu ted to e rrors introduced b y the simulation kernel's pro cessing order of CDR message relay events.

The most likely source of these collisions is caused by the transmission pipeline's placement of si mulated bit errors within each   packet. These bit errors are partially determined by the software's pseudorandom number generator, so if there were slightly overlapping transm ission sim ulation events   that occurred regularly throughout the scenario, then it would be possible for the network to only experienced a small number of unrecoverable bit errors, due to the specific pl   acement of each bit er ror within cer tain simulated transmissions.

Nonetheless, it is not surprising th   at both the SINCGARS and the EPLRS networks were able to support the application being run during this scenario. The results of both networks area presented in greater detail in the following two sections.

a.   SINCGARS Performance

Our SINCGARS network yielded a 100% success rate in message delivery by all nodes transm itting across the network. Of   the 4475 total traffic m essage events that were created during the 15 hours of si   mulation tim e, e very m essage was delivered successfully. This performance was expected, because all radios were transmitting at the same constant rate and each rad   io started th eir transm issions at staggered sim ulation times, ensuring that no two radios would be transmitting simultaneously.

During this scenar io, n either the tr ansmission nor the r eception ra tes at each SINCGARS node ever went above 624 bits per second. As shown in Figures 10 and 11, they both have an average throughput of around 300 bps , which is well below the 16 Kbps maximum data rate of the radio. These figures will be used for comparison to those generated by other simulation runs discussed later in this chapter.
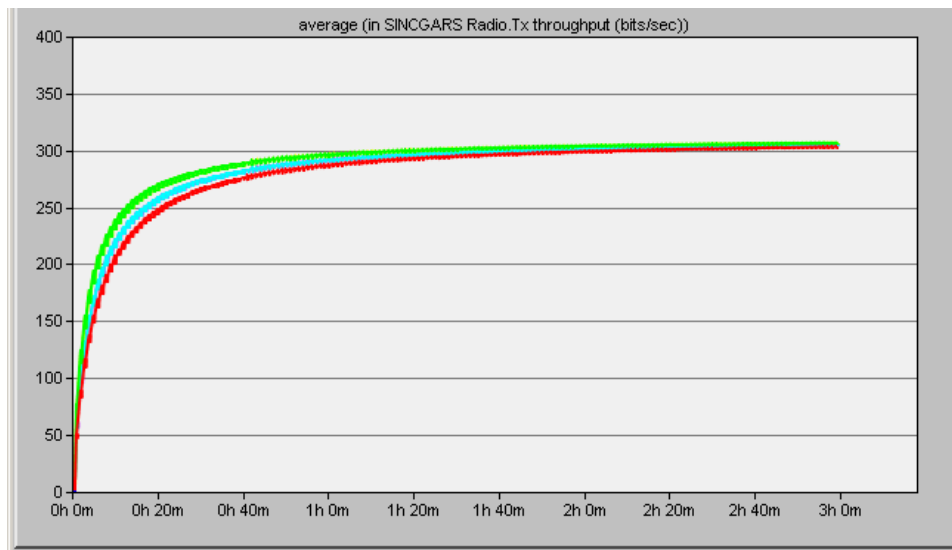

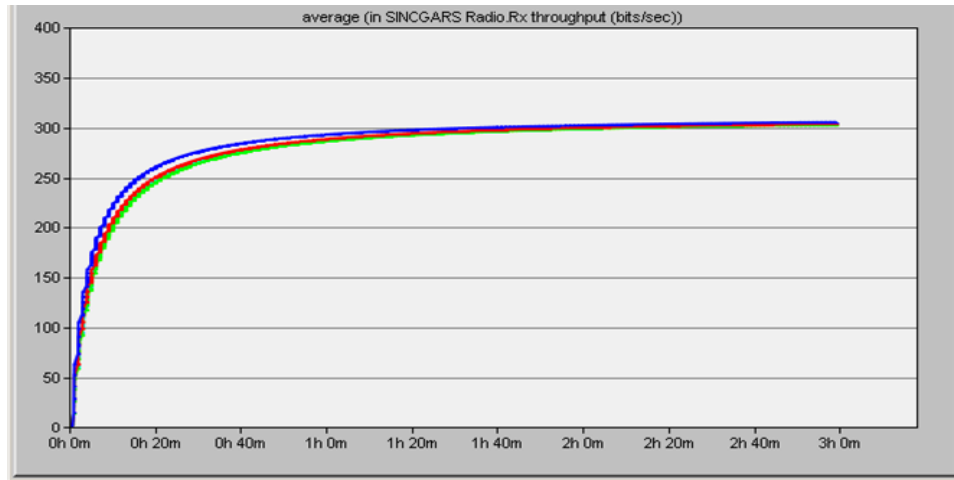Figure 10.   SINCGARS Platoon (Position Only): Average Tx Throughput

Figure 11.   SINCGARS Platoon (Position Only): Average Rx Throughput

b.   *EPLRS Performance*

Our EPLRS network also yielded a   100% message delivery success rate during this simulation scenario. Of the 4475 tota l traffic message events that were create during the 15 hours of sim   ulation tim e, every m essage was delivered successf ully. Again, this is not entire ly unexpected, because each radio transmitted their messages at the same constant rate, ensuring that no two radios would be transmitting simultaneously.

The transmission and reception rates at each EPLRS node never go abo ve 250 and 355 bps, respectively. Figures 12 and 13 show that the average transm   it throughput of four of the nodes was roughly 45 bps and the average receive throughput of the same four nodes was between 43 and 45   bps at. Both the Gateway node and MTR Squad node average throughputs vary noticeably from the other four nodes.

Since the Gateway did not originate any application traffic, it rarely blocked the transmissions from other nodes by attempting to transmit itself, so its receive throughput m easured higher than all of the ot   her nodes in the networ k (the top line in Figure 13). W e do notice, however, that th e Gateway does transmit a sm all amount of traffic (bo ttom line in Figure 12   ). This is s imply the E PLRS device comm unicating routing inform ation to its neighboring devices, and de   monstrates the sm all a mount of network overhead required for the maintenance of even simple EPLRS networks.

The MTR node transm its m uch less data than the other non-Gateway nodes on the network (second line from the botto m in Figure 12). This is because this node is further away from the other nodes th an the Gateway node. Since the Gateway node is the destination for all application traffic generated during this scenario, the MTR node knows that it is no t as close to the other nodes as the gateway, so it chooses not to relay any of the other nodes' transm issions. Since the four other nodes are roughly the same distance away from the Gateway, they most likely attem pt to relay m ost of each other's transm issions to the Gateway, which explains their alm ost identical average transmission throughputs (lines overlapping at the top of Figure 12).

Regardless of the differences between each of the nodes, all of these rates are well below the 51.83 Kbps m aximum achievabl e data rate of our CSMA needline. These f igures will be u sed f or comparison to those genera ted by other sim ulation runs discussed later in this chapter.
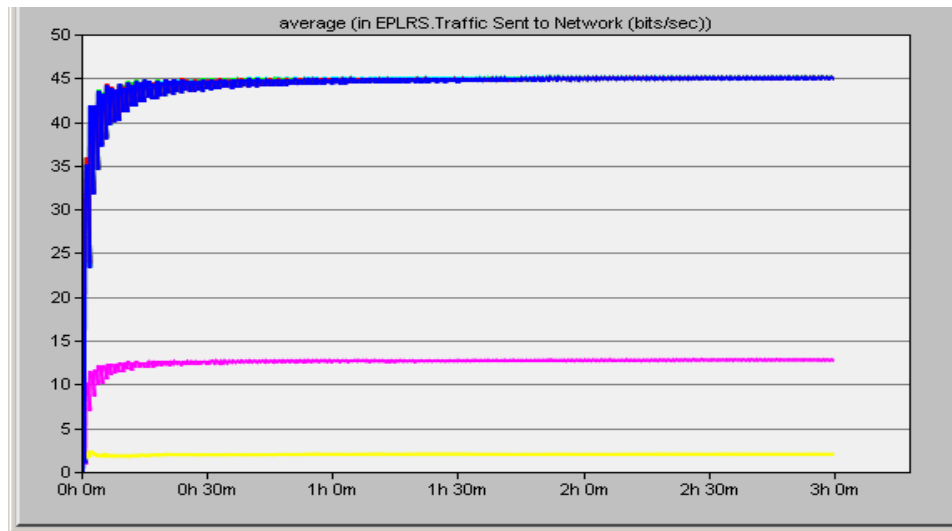

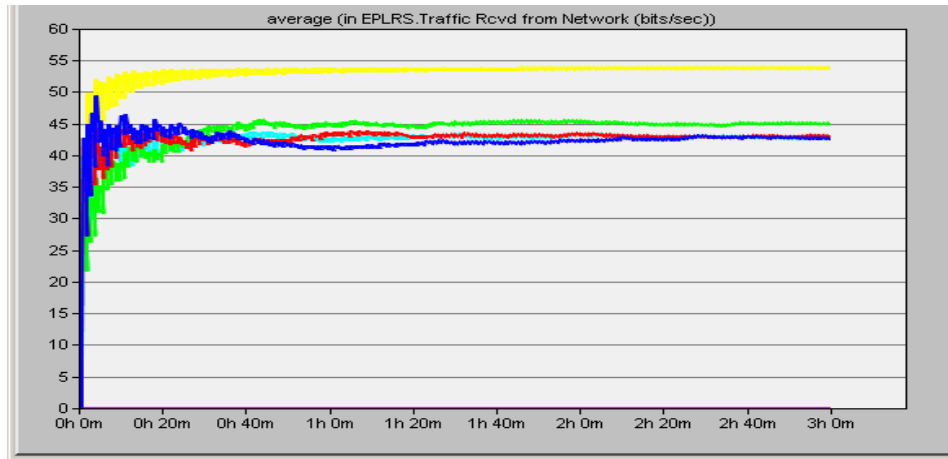Figure 12. EPLRS Platoon (Position Only): Average Tx Throughput

Figure 13.   EPLRS Platoon (Position Only): Average Rx Throughput

Notice that the SINCGARS network av eraged an ov erall s ignificantly higher transmit and receive th roughputs than the EPLRS ne twork. These differences are due to the higher throughput of the EPLRS de vice. Since the transm ission rate of the EPLRS is much higher than that of the SINCGARS, it spend s more time sitting idle than the SINCGARS radio, which m eans that under the sam e traffic con ditions, over any period of tim e the longer id le times will br ing down the throughput utilization averages. This does n ot mean that the nodes on the EPLRS network transm itted fewer or sm aller application messages.

2.   Short Message Only

Only the C DR and SINCGARS networks we re able to successf ully support this simulation scenario. The CDR and SINC GARS networks achieved 99.6% and 99.9% delivery success rates, respectively, and the EPLRS network achieved a 60.2% delivery success rate, demonstrating the EPLRS surprising inability to support this scenario using the CSMA needline.

In the CDR network, the resu lts p resented in [1] show that no m ore than tw o retransmissions were required across the 15-hour sim ulation, with only 3 m essage transmissions taking longer than about a second (but no more than 3 seconds). It required between one and two retransm issions per hour and saw an a verage TCP latency of 0.408 seconds.

The results of the SINCGARS and EPLRS   networks area presented in greater detail in the following two sections.

a.   SINCGARS Performance

Our SINCGARS network yield ed a 99.9% m essage delivery success rate by all nodes attached this network.   Of the   1756 traffic total m essage events that w ere created, only two m essages were n ot delivered successfully. Even tho ugh this scenario produced less traffic th an the Position Upda te Only scenario, because each node was generating m essages of greater size (160 Byte   s versus 50 Bytes) at random   intervals, instead of smaller messages at constant, offset intervals, it is not surprising to encounter a small number of collisions caused by simultaneously generated transmissions.

Despite the larger m   essage size and the greater am   ounts of overhead network traffic caused by the use of TCP m   essages for this applica tion's transmissions, Figures 14 and 15 show that the average   transmit and the rece ive throughputs actually show minor decreases from those seen in the previous scen ario. This is likely a res ult of the lower q uantity of messages tran smitted acro ss the ne twork in th is scenario, causing the increased amount of idle time for each radio to lower the overall average throughputs.
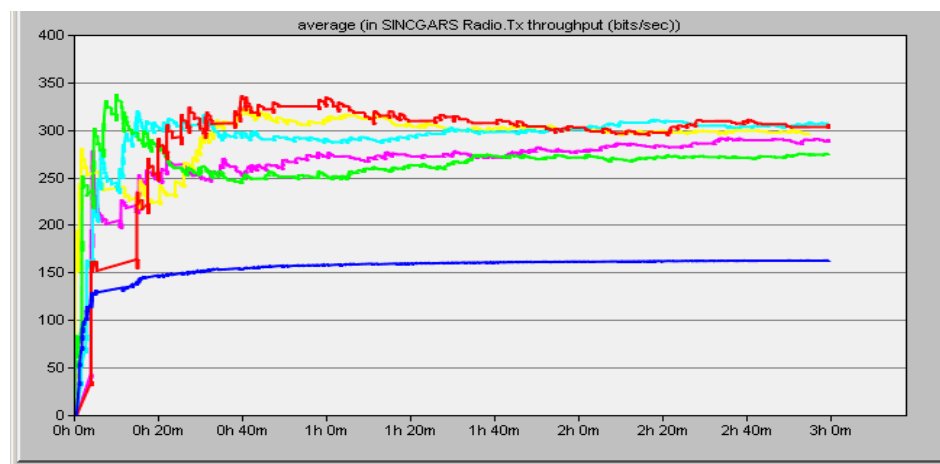

Figure 14.   SINCGARS Platoon (Short Message Only): Average Tx Throughput
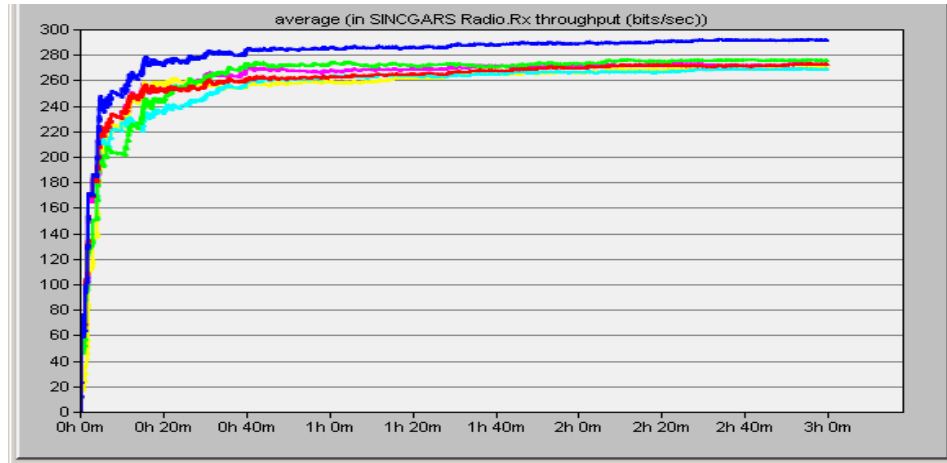
59

Figure 15.   SINCGARS Platoon (Short Message Only): Average Rx Throughput

As shown in Figure 16 and 17, the average TCP delay was 0.772 seconds (almost twice as long as the CDR TCP la   tency of 0.408 seconds) and, there were approximately 6 TCP re transmissions per hour (three times that of the CDR), with only two transmissions that needed to be retransmitted twice.
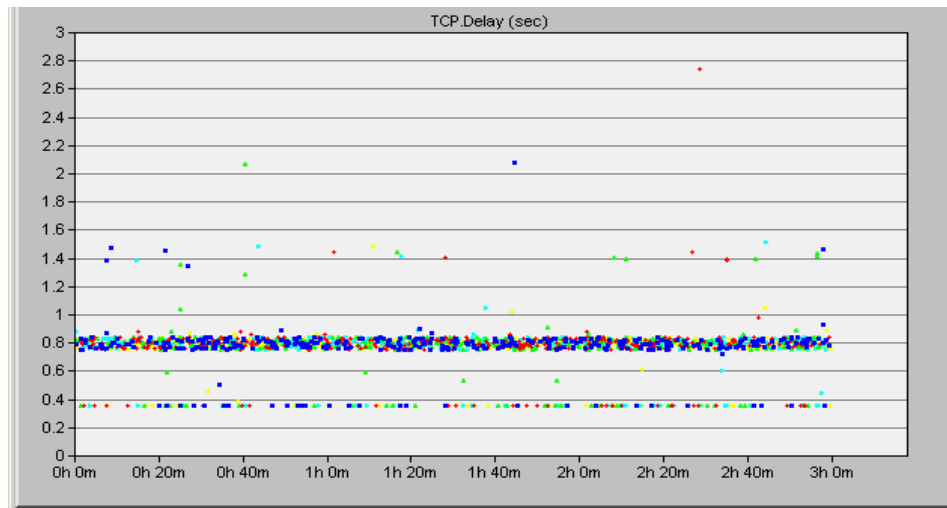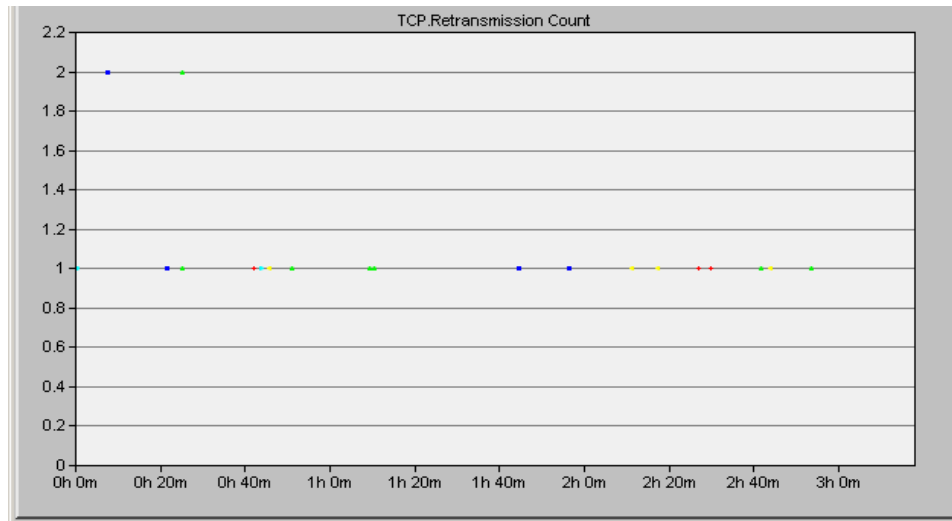

Figure 16.   SINCGARS Platoon (Short Message Only): TCP Delay

Figure 17.   SINCGARS Platoon (Short Message Only): TCP Retransmission Count

b.   EPLRS Performance

Our EPLRS network had an overall m   essage delivery success rate of 60.2% during this simulation scenario. Of the 1,653 total traffic message events that were created, 658 m essages were not delivered su   ccessfully. This was significantly less successful than both the SINC GARS and CDR networks, and   would not be acceptable performance metrics for use by actual military units.

As depicted in Figures 18 and 19, we   see that the average transm ission rates for each node range between 120 and 140 bps, and the average reception rates range between 170 and 225 bps. This is roughly four   times greater than th at of the Position Update Only scenario, but still well belo   w the 51.83 Kbps m   aximum data rate of our CSMA needline. Again , we see a noticeab le d ifference between the amount of traffic sent and received by the MTR Squad (bottom line in Figure 19 and 20) and the rest of the nodes. This is caused b y the sam e reasons as those m entioned in the Position Up date Only scenario discussion.
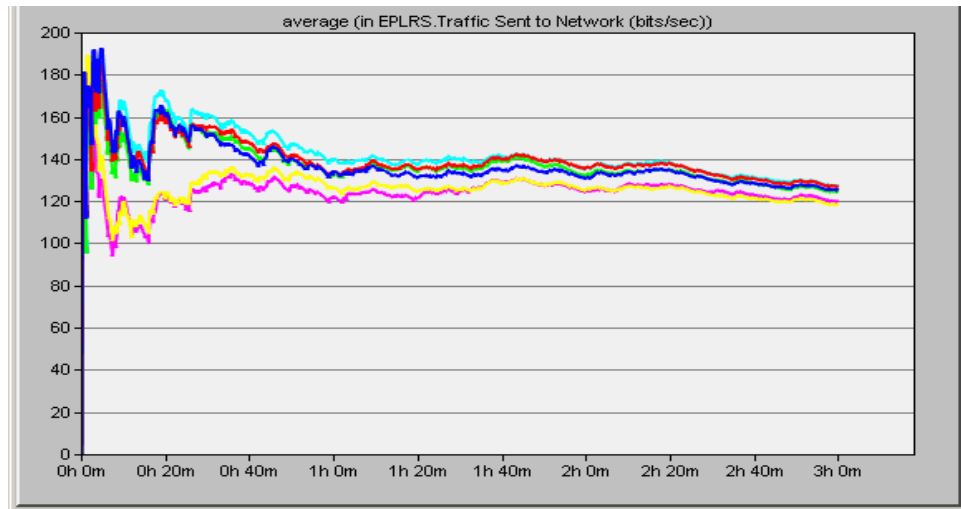
Figure 18.   EPLRS Platoon (Short Message Only): Average Tx Throughput
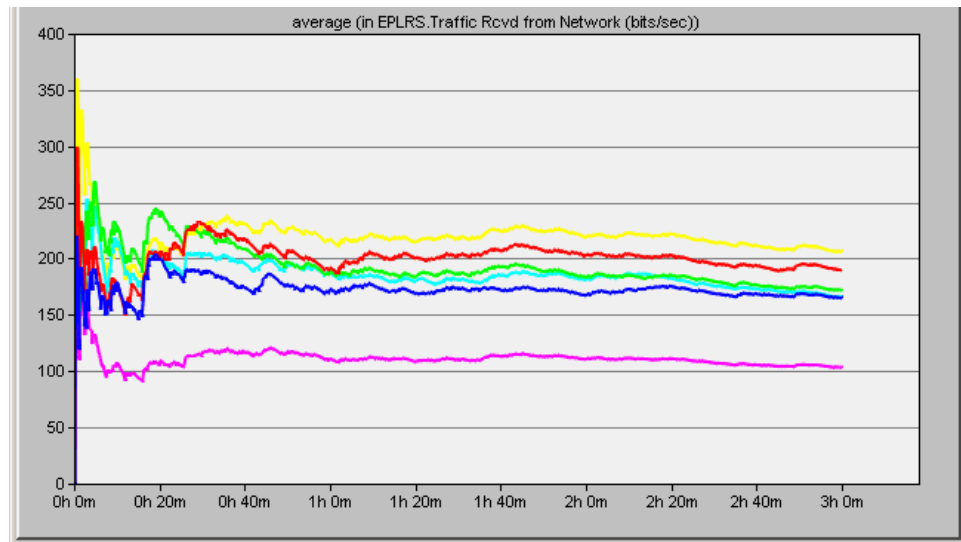

Figure 19.   EPLRS Platoon (Short Message Only): Average Rx Throughput

As shown in Figure 20, the average   TCP delay had a m aximum delay of 76.813 seconds, and averaged 1.1472   seconds, which is almost three times greater than the 0.408 second average delay for the CDR network.

Figure 21 shows that there were signi   ficantly more TCP r etransmissions than in the SINCGARS. The average   retransmission count was 2.75 (SINCGARS averaged 1. 25), with a peak co   unt of   12 attem pts. The increased num   ber of retransmissions is m ost like ly due to the re being a high num   ber of instances where

multiple nodes were attempting to introduce tra ffic at the same time. Remember that the EPLRS CSMA needlin e m ulti-hop im plementation forces each node to delay their transmissions until the previous ly transm itted s ignal has h ad the chan ce to trave l the maximum number of hops. Since each node att ached to the CSMA nee dline is forced to wait until the same time after each transmission and transmission relay before introducing new traffic (for a 6 hop networ k the transmission orig inator waits 5 time slots, th e first relay node waits 4 time slots, etc.), the chances of multiple nodes attempting to introduce traffic immediately at the end of t his CS MA needline im posed wait period are fairly good. Since there was no forced wa it time for t he SINCGARS node transm issions, this may account the fewer number of transmission collisions.
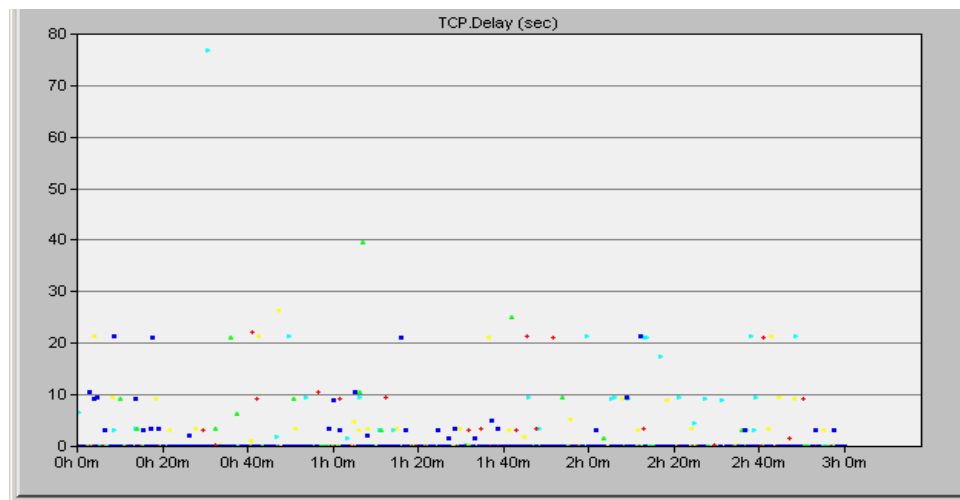

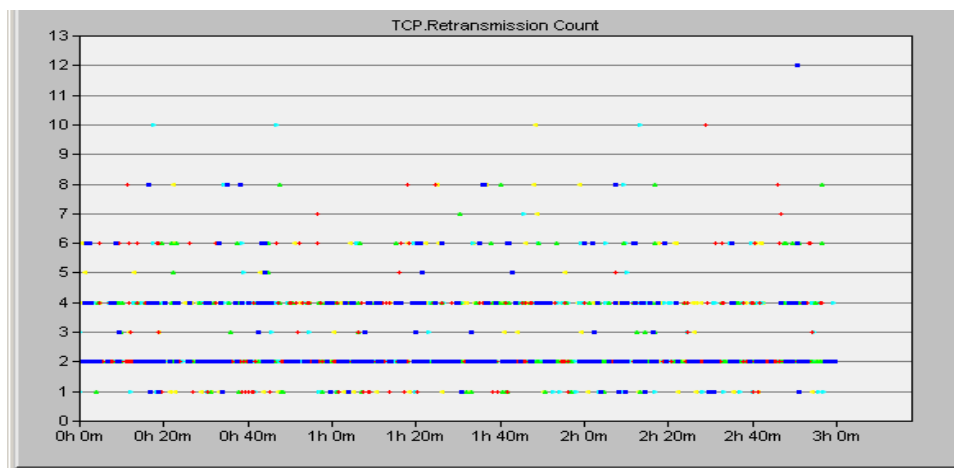Figure 20.   EPLRS Platoon (Short Message Only): TCP Delay

Figure 21.   EPLRS Platoon (Short Message Only): TCP Retransmission Count

63

In Figure 22, we show data from three separate EPLRS nodes representing the amount of traffic each node is introducing into the netw ork (the top three lin es) and the amount of traffic being generated by app lications runn ing at each no de (the botto m three lines). For each of these nodes, the am ount of traffic being tran smitted across the network is roughly four tim es as great as the traffic bein g generated, illus trating the increased traffic load created by using TCP, relaying other nodes' transm issions, and the small amount of overhead involved in each nod e maintaining its rou ting information for the network.
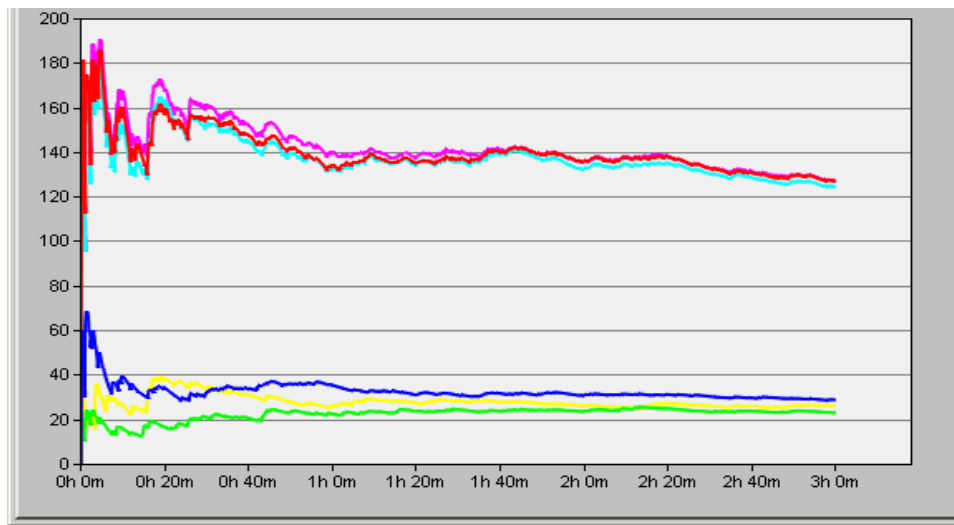

Figure 22.   EPLRS Platoon (Short Message Only): Relay vs. Non-Relay Traffic

We ran this sim ulation again using UDP, instead of TCP, a nd of the 1745 total UDP messages, all but two messages were delivered successfully (a 99.89% success rate). Obviously, the additi onal ov erhead incurred by the use of TCP had a significant impact on the effectiveness of this network.

Aside from switching our applicati on's m essages from TCP to UDP, it might be also possible to use different need line configurations of the EPLRS device to achieve acc eptable resu lts f or sim ilar tra ffic loads across an EPLRS network (i.e., reducing hop count or altering waveform type), but that will be left to future work.

3. Commanders and Position

A summary of each network's perform ance under this scenario is shown in Tab le 4. Surprisingly, only the SINCGARS network was able to fully support all five node applications, despite it h aving the lowest overall transmission rate of the three netw ork devices. The results presented in [1] show that the CDR ne twork easily supported three of the applications, but failed to provide adequate HTTP and Email support. The EPLRS provided better HTTP and Em ail support than the CDR, but at the expense of the other three applications. The results of the SINCGARS and EPLRS networks area presented in greater detail in the following two sections.

%	CDR	SINCGARS	EPLRS
Position Update	99.5	100	94.49
Short Message	100	98.13	66.73
IRC	100	100	86.95
HTTP	39	100	55.83
Email	39	100	55.83

Table 4. Commanders and Position Application Success Rates (Platoon).

a. SINCGARS Performance

Our SINCGARS network running the Commanders and Position scenario achieved the highest success rate in message delivery by all nodes tran smitting across the network. Of the 17412 total traffic m essage events that were created, only 19 messages were not delivered successfully. However, it is worth mentioning that this sim ulation did not include the introduction of normal tactical voice traffic, which would have surely degraded these perform ance results signifi cantly, since the radio does not effectively support simultaneous transmission of both data and voice across a single channel.

Under this scenario's network load, we see that both the transm ission and reception rates in crease, as expected with th e introduction of additiona l network traffic. Since all of the additional traffic is between the Gateway and Platoon Commander nodes, we notice that the transm ission rates of th e Squad Leader nodes do not increase, but the

amount of t raffic introduced onto the netw ork by the Gateway (top line) increases to almost 5 times that of the other nodes. Additionally, the amount of traffic received by all of the other nodes triples, as displayed in Figures 23 and 24.
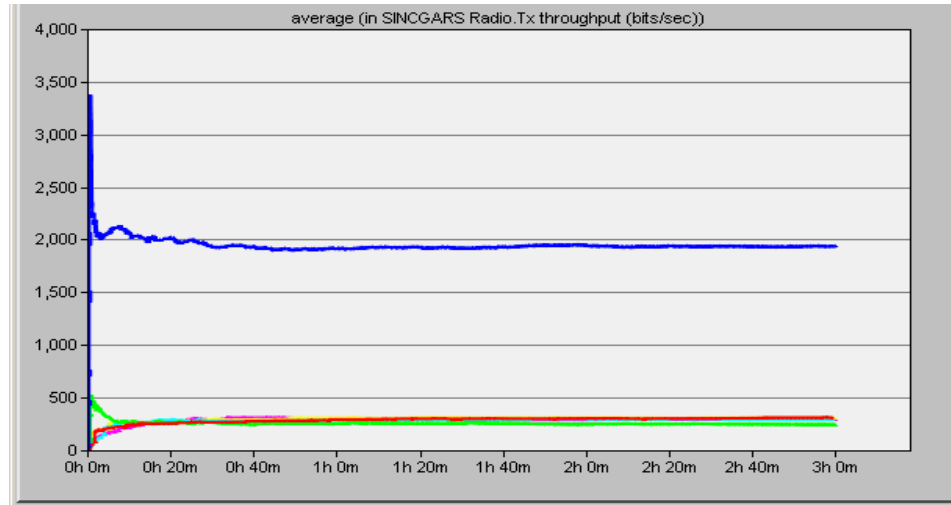

Figure 23.   SINCGARS Platoon (Commanders & Position): Average Tx Throughput
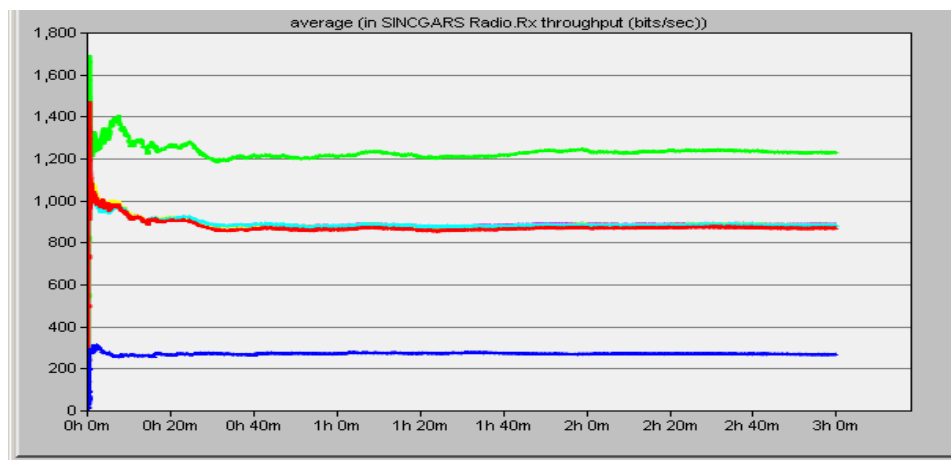

Figure 24.   SINCGARS Platoon (Commanders & Position): Average Rx Throughput

Overall, the TCP statistics reflect th e impact of increased network traffic, showing increases in delays and retransm ission counts. Figure 25 and 26, show that the average TCP delay was 1.12 seconds, alm ost double what was experienced in the Short Message Only scenario, and the averag e TCP retransm ission count was 1.27, only slightly higher than the previous scenari o, with none being retransm itted m ore than 4 times (double the previous maximum retransmission count of 2 times).
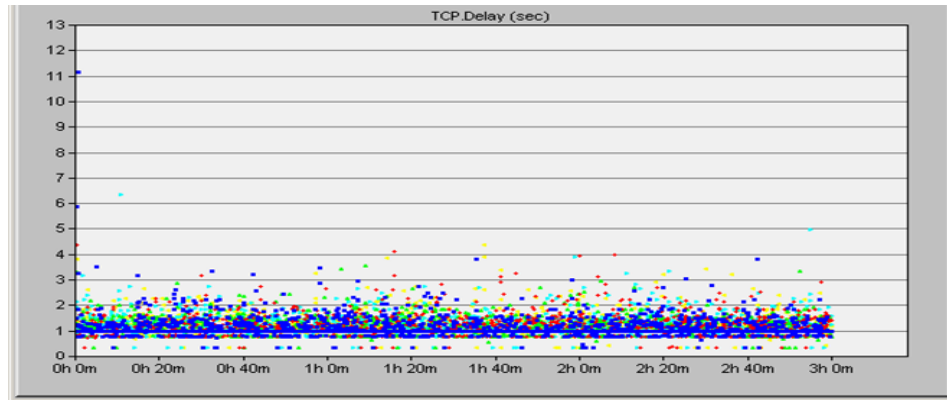
66

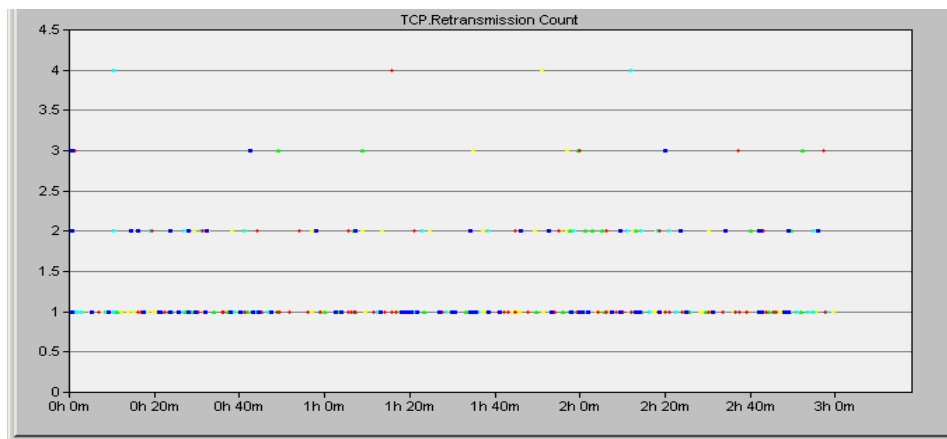Figure 25.   SINCGARS Platoon (Commanders & Position): TCP Delay

Figure 26.   SINCGARS Platoon (Commanders & Position): TCP Retransmission Count

b.   EPLRS Performance

While the EPLRS network in this s   cenario showed slig htly im proved Short Message application success rate (more than 6 percent higher), it still did not come close to being able to ade   quately support four of the fi   ve applications, the exception being the Position U   pdate application.   The reason we saw this change in the performance of the Short Message applic   ation was due   to different pseudorandom numbers controlling the actua l transm ission tim ing of each   of these m essages. Even though each sim ulation run was started with   the same seed as those fro m the previous scenarios, since there are m   ore applica tions using the sam   e pseudorandom number generator to determine their transm ission times, the transm issions that occur later in the simulation will be triggered by different numbers than they were in the previous scenario.

67

This is one quirk of using software-based simulations, which is discussed in greater detail in [15] and [16], and is not   intended to im ply that th e throughput of one application should increase with greater overall resource demand.

Under this scenario's network load, we see that both the transm ission and reception rates in crease, as expected with th e introduction of additiona l network traffic. Since all of the additional traffic is between the Gateway and Platoon Commander nodes, we notice that the transm ission rates of the Squad Leader only double, but the am ount of traffic introduced onto the network by the Gatewa y increases to almost four times that of the other nodes. Additionally, the a   mount of traffic received by the Squad Leaders double and the a mount received by the Gateway and MTR Squad increase by a factor of 10, as shown in Figures 27 and 28.
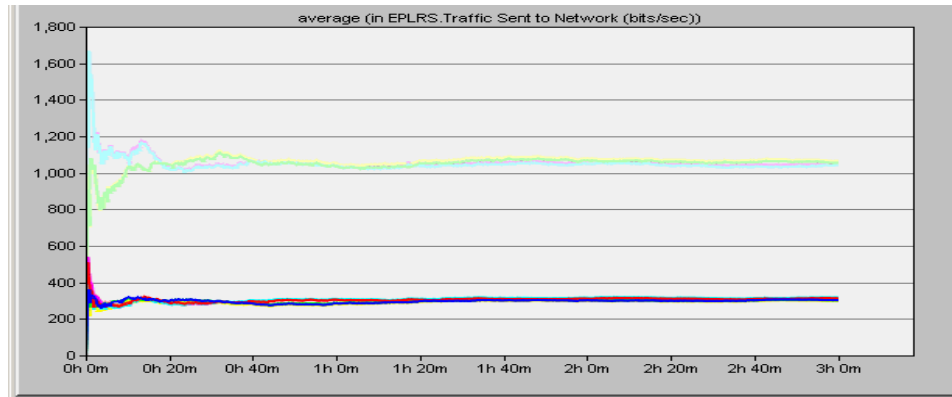

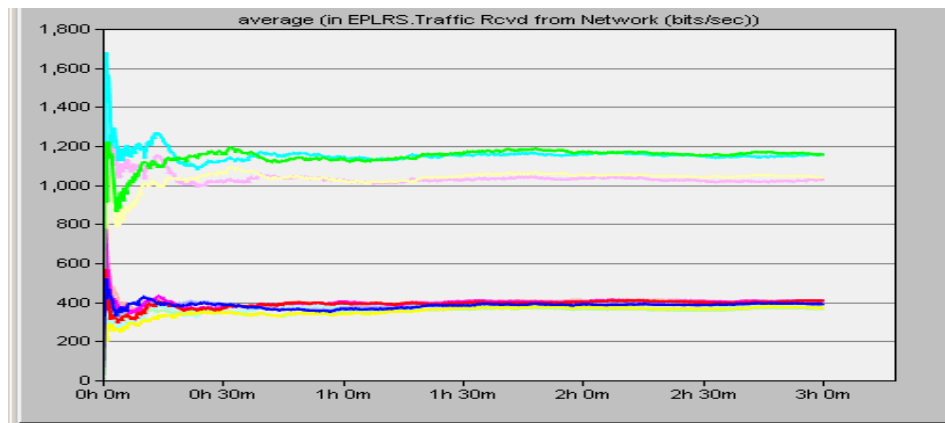Figure 27.   EPLRS Platoon (Commanders & Position): Average Tx Throughput

Figure 28.   EPLRS Platoon (Commanders & Position): Average Rx Throughput

Overall, the TCP statis tics ref lected the im pact of increa sed networ k traffic, showing increases in delays and re transmission counts. As shown in Figure 29, the average TCP delay was 0.321 seconds for all but one of the sim ulation runs for this scenario. F igure 30 shows that one of our si mulation runs achieved TC P delays of over 6000 seconds. That is a delay of over 100 m inutes, which would be entirely too long for any of the applications running across our network.

The long delay seen in this sim ulation run was probably caused by one node's transmit queue becoming backed-up to a level that causes significant delays. Since we are assuming that there is no m aximum holding time limit for a single node to utilize the CSMA needline, once a node has the needlin e, it will not let it go until it has em ptied its transm it queue. This m eans that there is a chance of a single node having to wait indefinitely for access to the need line resou rces. This circu mstance is m itigated in real life by the E PLRS "maximum hold tim e" setting, which se ts a ce iling for the amount of time one single node can m aintain control ove r a single needline's network resources. Because this setting was not available for our JCSS EPLRS model, we s ee one potential result of having the maximum hold time set to infinity.

Figure 31 s hows that the averag e TCP retransm ission rate was 2.24 (almost twic e that of the SINCGARS network), with a m ajority of tran smissions being retransmitted between 1 and 6 tim es. Th e m aximum retran smission count of 15 retransmission attempts was almost four tim es greater than the m aximum count from the SINCGARS network.
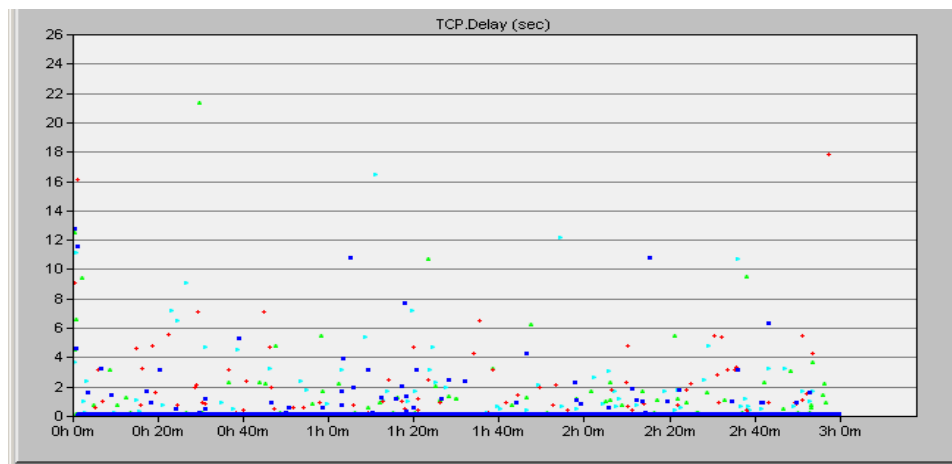

Figure 29.   EPLRS Platoon (Commanders & Position): TCP Delay
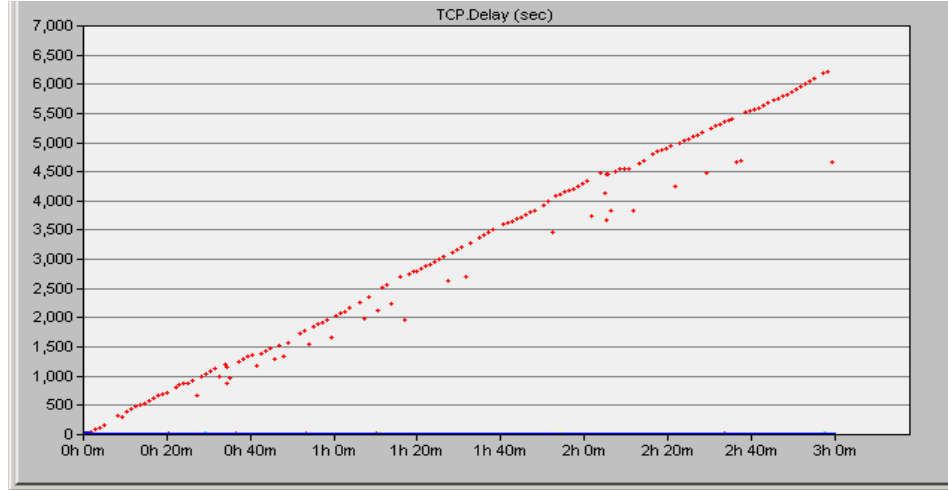
69

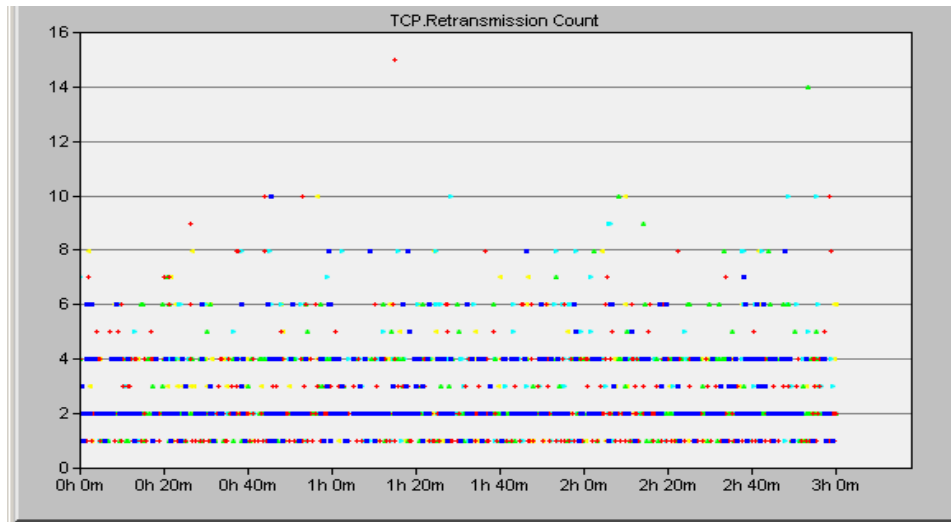Figure 30.   EPLRS Platoon (Commanders & Position): TCP Delay

Figure 31.   EPLRS Platoon (Commanders & Position): TCP Retransmission Count

4.   Currently Deployed Applications

A summary of each network's perform ance under this scenario is shown in Tab le 5. Using the results presented in [1], we s ee that only the CDR network was able to fully support all three applications. This is m   ost likely because of its use of cooperative diversity, which allows each node to interpret multiple instances of the same transmission as a single transm ission, that is, to m itigate collision s by treating id entical receip ts as 'non-colliding transm issions. Since both the Position Update and Video applications produce a high volume of regularly transm   itted m essages, the lik   elihood of these

70

transmissions (and their respective relays) col liding with each other is h igh. The ability of the CDR to overcome these types of tran smission co llisions and successfully allow these messages to be delivered is evident when considering the simulation results.

Overall, the SINCGARS network was m arginally able to suppor t the applications run in this scenario, and the EPLRS ne twork failed to support all but the Video application. The resu lts of the SINCGARS a nd EPLRS networks area presented in greater detail in the following two sections.

%	CDR	SINCGARS	EPLRS
Position Update	99.6	100	24.24
Short Message	99.6	72.11	60.58
Video	99.9	80.7	98.66

Table 5.   Currently Deployed Applications Application Success Rates (Platoon).

a. SINCGARS Performance

Our SINCGARS network was only able to support the Position Update application during this sim ulation scenario. Ho wever, it is a little su rprising that none of the Position Update m essages collided with the Video application transm issions. Since both applications are generating constantly spaced transm issions, Video once every 0.5 seconds and Position Update once ev ery minute for each nod e, it would seem likely that at least one Position Update m essage would run into on e of the 21600 video m essages, especially s ince both applica tions are set to begin their transmissions at the very beginning of a sim ulation-time second. The si gnificant decrease in support of the Short Message ap plication is likely due to incre ased traf fic collis ions with the constantly streaming Video application.

Under this scenario's n etwork load, Figures 32 and 33 show that the average tran smission throughput for each rad io rem ains ro ughly th e sam e, where the reception throughput almost doubles. Since th e only the g ateway node has an increased

71

transmission burden of sending the Video appl ication messages, it m akes sense th at the reception throughputs of the other nodes increases, since all other nodes will be receiving more data when sitting idle.
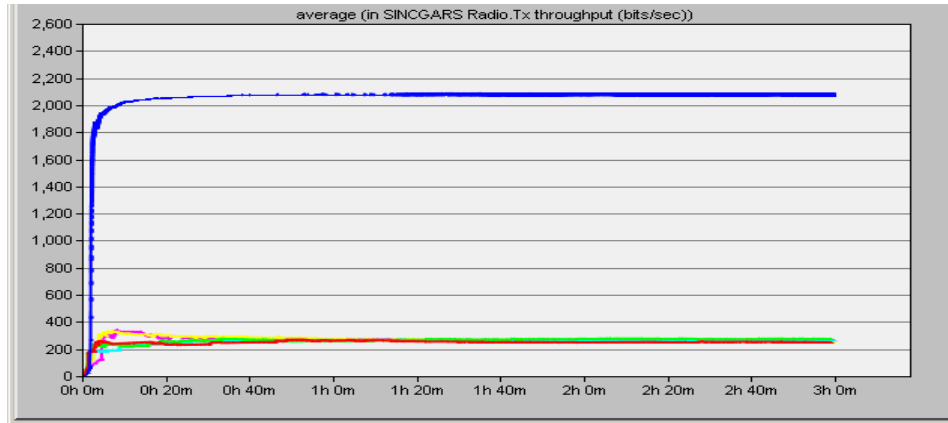

Figure 32.   SINCGARS Platoon (Current Applications): Average Tx Throughput
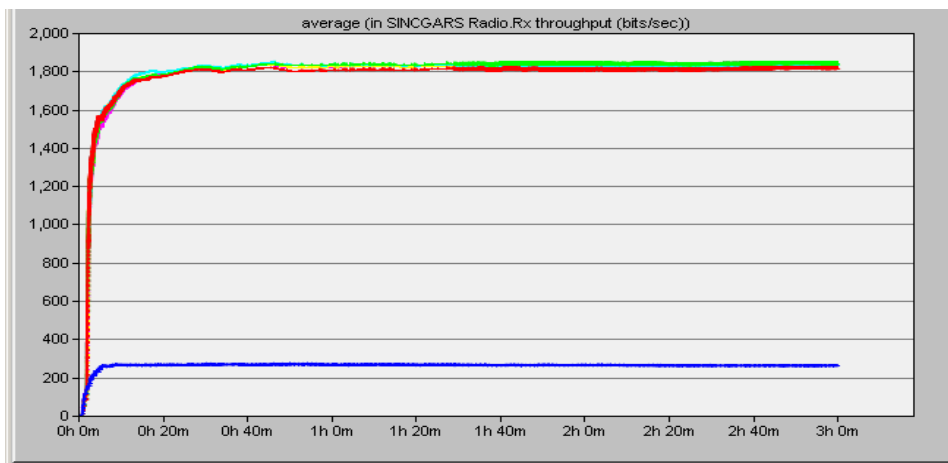

Figure 33.   SINCGARS Platoon (Current Applications): Average Rx Throughput

Overall, the TCP statistics ref lected the im pact of the incre ased networ k traffic, showing increases in delays and re transmission counts. As shown in Figure 34 and 35, the average TC P delay was 1.96 seconds—alm ost double what was experienced in the previous scenario by this network,   but the m aximum TCP delay decreased from 11.15 seconds to 8.51 seconds. The average T   CP retransm ission count was 1.29, only marginally higher than the previous scenario, with a maximum TCP retransmission count of six retransmissions.
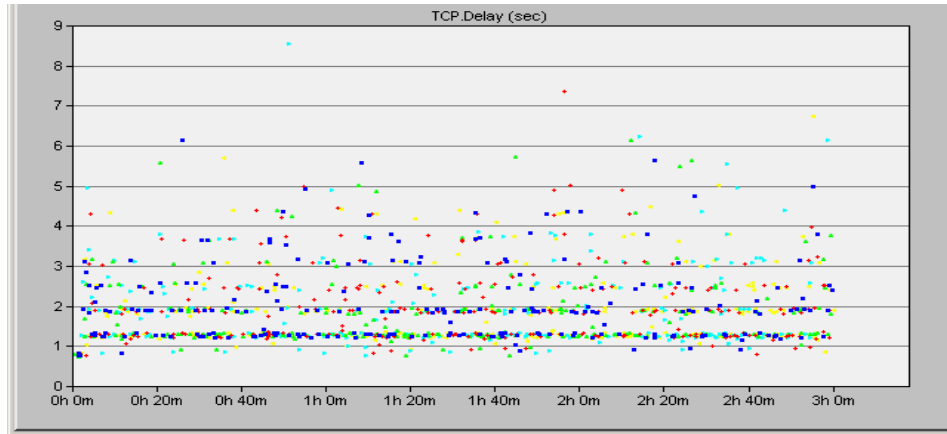
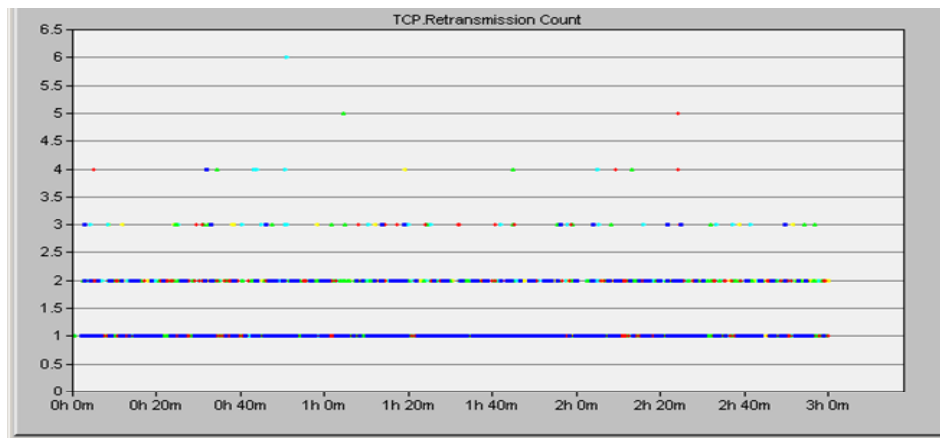Figure 34.   SINCGARS Platoon (Current Applications): TCP Delay

Figure 35.   SINCGARS Platoon (Current Applications): TCP Retransmission Count

b.   *EPLRS Performance*

The EPLRS network running the Current Applications scenario was only able to successfully sup port the Video application and failed to support both the Position Update and Short Message a pplications. The decrease from   94.49% to 24.24% of the Position Update su ccess ra te was enorm ous, and is   rep resentative o f how incre ased network loa ds can dras tically af fect the pe rformance of a   networ k that does little to ensure qu ality of serv ice. W ith th e hi gh rate of Video application m   essages being introduced onto the n etwork, it is   not surp rising that m any of the Position Up   date messages would collide with some number of the 21 ,600 video messages being broadcast during each simulation.

73

The decrease in success rate for the Short Message application droppin g back down to 60.58% is not surprising, sin ce in this scenario none of the other applications use the pseudo randomly generated transmission tim es. This is alm ost the exact sam e success rate as th e Sho rt M essage Only scenario, and is likely due to the similarly timed message collision s occurring in this s cenario as the Sho rt Message Only scenario.

Under this scenario's n etwork load, Figures 36 and 37 show that the average transmission throughput for each radio increases to alm ost ten tim es higher than the previous scenario. T his dem onstrates the effect relaying communication nodes can have on overall network load. As the num ber of generated m essages across the networ k has increased, so does the num ber of m essage relays sent across the network, which increases the am ount of tota l network transm issions. Si nce the Video application introduces a significantly greater amount of tr affic, we should expect the overall network throughput to increase accordingly.
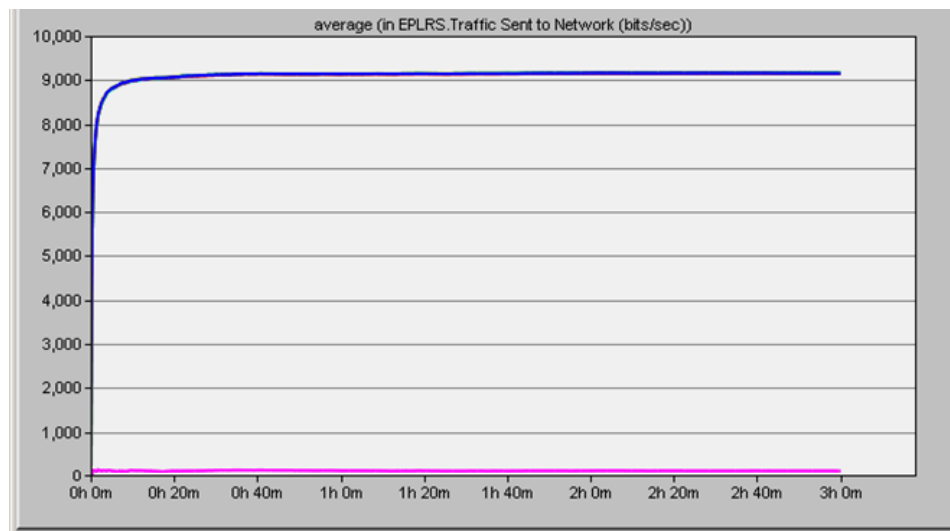

Figure 36.   EPLRS Platoon (Current Applications): Average Tx Throughput
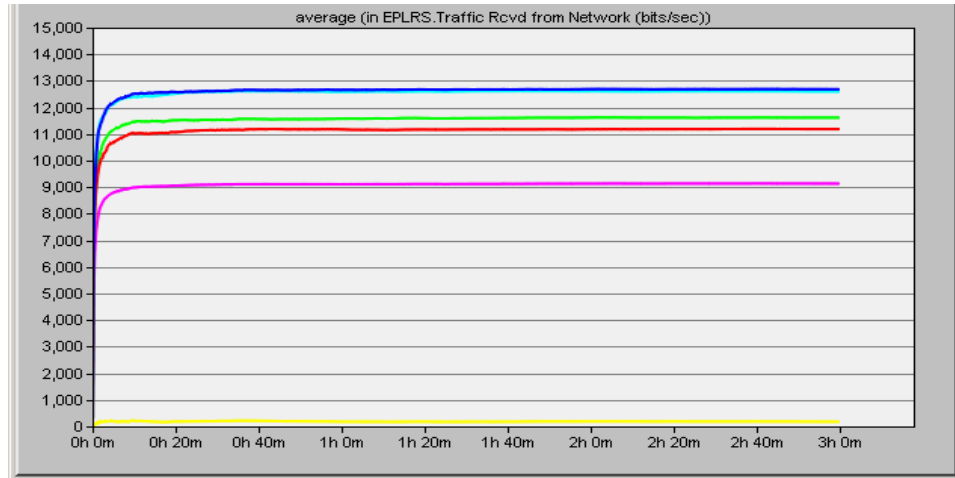
Figure 37.   EPLRS Platoon (Current Applications): Average Rx Throughput

Overall, the TCP statistics reflected the impact of increased network traffic, showing longer delays and higher retransmission counts. As shown in Figure 38 and 39, the average TCP delay was 2.22 seconds, almost eight times the delay experienced by the same network in the previous scenario, and the maximum TCP delay increased from 22 seconds to 75 seconds (not considering the anomalous 6206.2 second delay created by having an infinite maximum hold time setting). The average TCP retransmission count was 2.55, only slightly higher than the previous scenario, and had a maximum TCP retransmission count of 10 retransmissions (down from 15 in the previous scenario).
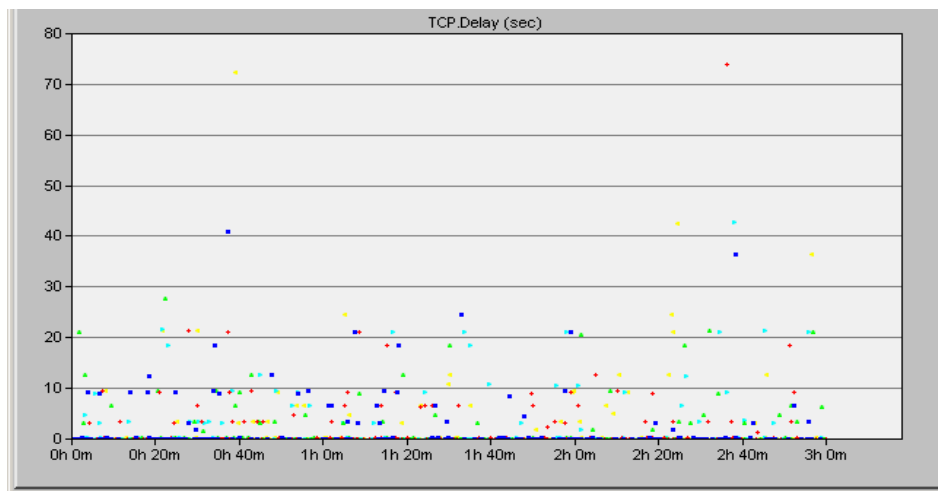

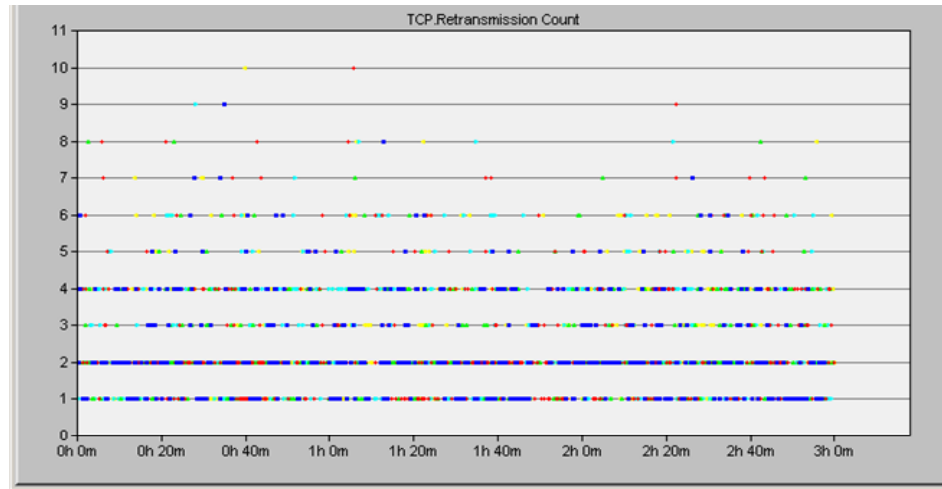Figure 38.   EPLRS Platoon (Current Applications): TCP Delay

75

Figure 39.　　　EPLRS Platoon (Current Applications): TCP Retransmission Count

5.　　　All Applications

A summary of each network's perform ance under this scenario is shown in Tab le 6. W hile the results presented in [1] show　that the CDR network failed to support the Email and HTTP applications, it significan　tly outperform ed both　the SINCGARS　and EPLRS networks during the simulation of this scenario.

Overall, the SINCGARS network failed to　provide simultaneous support to all of this scenario's applications. The EP　　　LRS network gave a generally m　　　ediocre performance, as well, even though it perfor　med noticeab ly better than th e SINCGARS. The results of the SINCGARS and EPLRS netw　orks area presented in　greater detail in the following two sections.

%	CDR	SINCGARS	EPLRS
Position Update	98.9	17.89	26.22
Short Message	99.6	74.2	62.87
IRC	100	8.67	95.5
HTTP	72	0.83	58.33
Email	39	0.83	58.33
Video	98.8	13.5	95.64

Table 6.　　All Applications Application Success Rates (Platoon).

76

a.   *SINCGARS Performance*

The perform ance of t he SINCGARS network during this sim ulation scenario was dism al at best. Its highest application m essage delivery success rate was 74.2% for the Short Message application, a nd it achieved a 99.2% fa ilure rate for the delivery of all HTTP and Em ail applicati on m essages. W ith a sudden increase in network resource dem and, the ability of th e SINCGARS network to support even one single application plum meted. Thi s further de monstrates the inability of a network that does not provide quality of service controls, such as CSMA or cooperative diversity, to support busy networks.

While the average transm ission a nd reception thro ughputs remain relatively unchanged from the previous scen ario, as displayed in Figures 40 and 41, the most noticeable d ifferences are in the TCP performance m etrics. F igure 42 shows that the average TCP delay increased from 1.96 seconds to 77.3 seconds, with a m aximum delay of 3809.4 seconds. This figure show s an alm ost e xponential increase in TCP delays, and does not show an increase in delay after about the one hour and twenty minutes point in the simulation, since the fi nal delay values for these m essages would have placed their d elivery well bey ond the dur ation of simulation run.   However, the average TC P retransm ission count was 1.27, surp risingly less than that of som e of the previous scenarios, as shown in Figure 43.
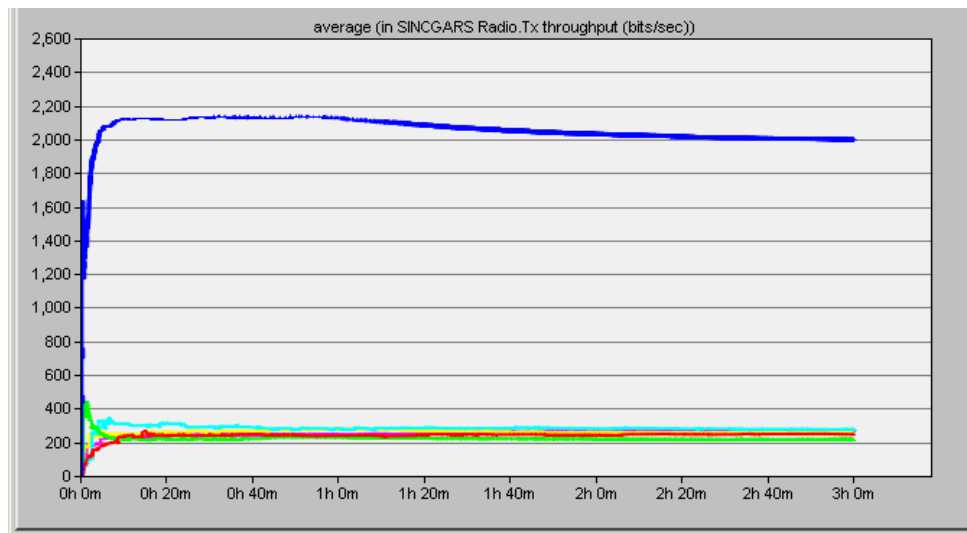
Figure 40.   SINCGARS Platoon (All): Average Tx Throughput
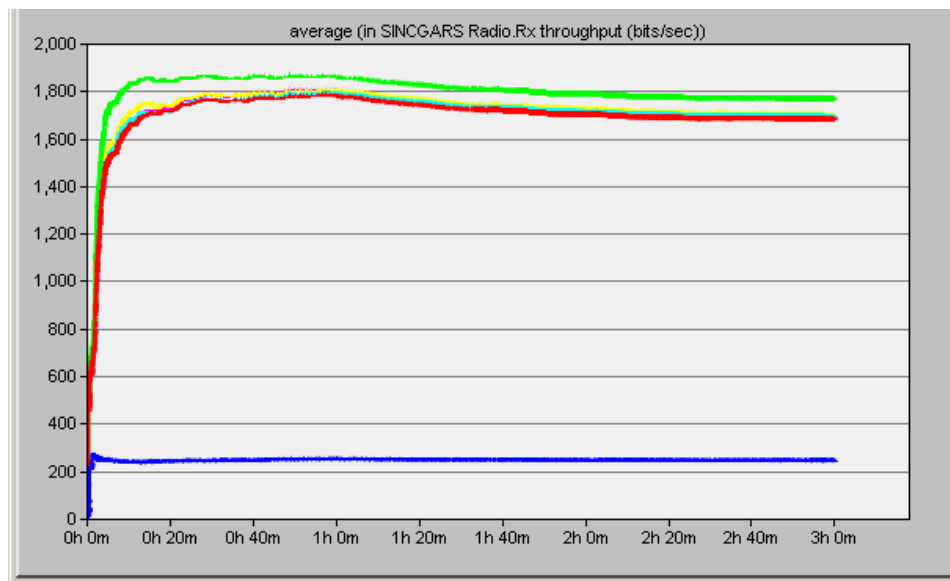

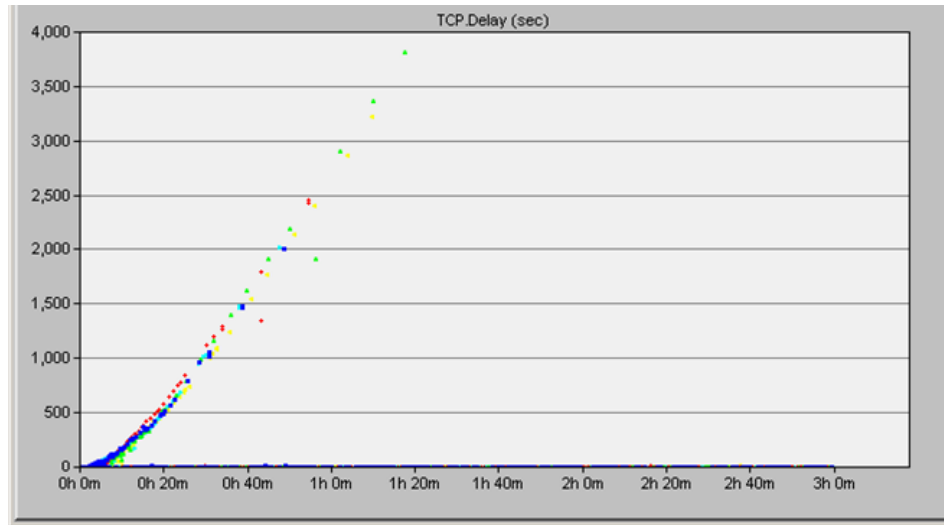Figure 41.   SINCGARS Platoon (All): Average Rx Throughput

Figure 42.   SINCGARS Platoon (All): TCP Delay

Figure 43.   SINCGARS Platoon (All): TCP Retransmission Count

The SINCGARS network's inability to   hand le this am ount of network traffic is du e to the la rge number of transm issions colliding with each other. Since e ach node will transm it as soon as it has traffic to   send, instead of waiting to transm it at the beginning of a ti me slot, it is very likely th at one node will interrupt th e transmission of another. In networks with hi gh traffic volume, the use of transmission time slots, such as the Slotted-ALOHA protocol in u se by the CD R model is preferred, b ecause it can help minimize the chances of transmission interfering with each o ther. If each node waits to

transmit new traffic at the beginning of a time slot, then their transmissions are less likely to collide with the tail end of a message that is already being transmitted by another node. Since the SINCGARS has no m ethod for m itigating these types of collis ions, we sho uld not be surprised at its poor performance during this simulation scenario.

b. EPLRS Performance

While the perform ance of the EPLR S network during this sim ulation scenario was better than that of the SINCARS, it also failed to adequately support all of the application traffic generated during this network load. Its highest app lication message delivery success rate was 95.64% fo r the Video application, which m ay se em good, but s ince ou r Video application is onl y tran smitting video at two fram es per second, such a degraded perform ance of an already less-tha n-poor-quality-video application cannot be considered a success.

While the average transm ission a nd reception thro ughputs remain relatively unchanged from the previous scenario, as shown in Figures 44 and 45, the most noticeable d ifferences are in the T CP performance m etrics. Figure 4 6 shows tha t the average TCP delay decreased from 2.22 seconds to 1.11 seconds from the EPLRS results in the previous scenario (even though th e maximum delay of 190.74 seconds was almost three times greater than in the previous scenario). While the average TCP retransm ission count was 2.54, shown in Figure 47, roughly the same as that of som e previous EPLRS scenarios, it is still m ore than double th at of the SINCGARS network during the sam e scenario, further illustrating the effects of increase collisions from transmission relays.
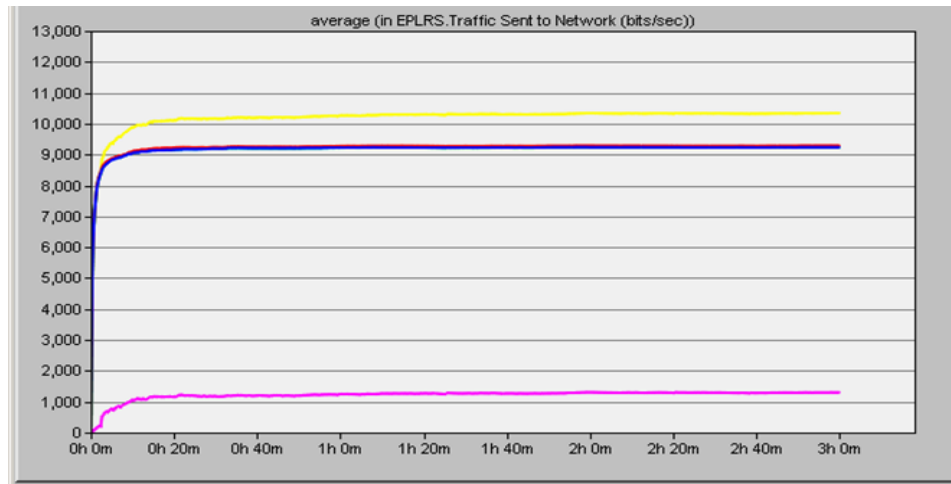
Figure 44.　　EPLRS Platoon (All): Average Tx Throughput
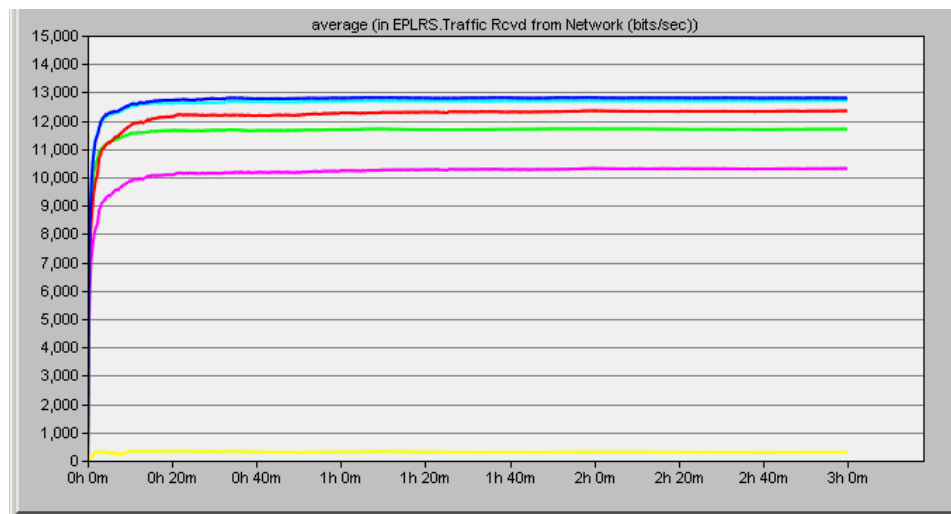
Figure 45.　　EPLRS Platoon (All): Average Rx Throughput

Figure 46.   EPLRS Platoon (All): TCP Delay

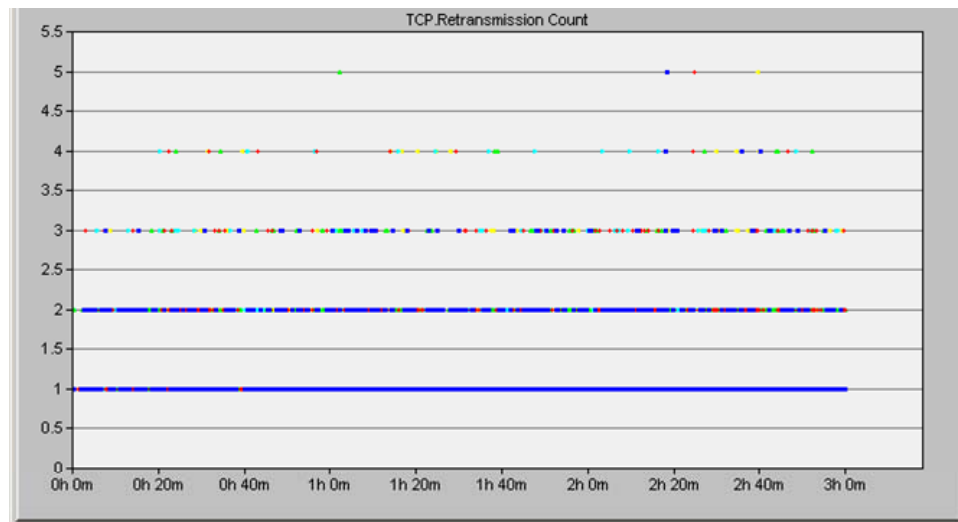Figure 47.   EPLRS Platoon (All): TCP Retransmission Count

C.   COMPANY SIMULATIONS

Our company-sized network sim ulations consist of twenty ra dios: three platoons identical to the one platoon from the previous set of scenarios, one m ortar platoon, one gateway node, one company executive office r, one com pany comm ander, one forward

observer, one JTAC, one UAV and one weapons platoon commander. Figure 48 depicts the location of each radio model within the simulated network.
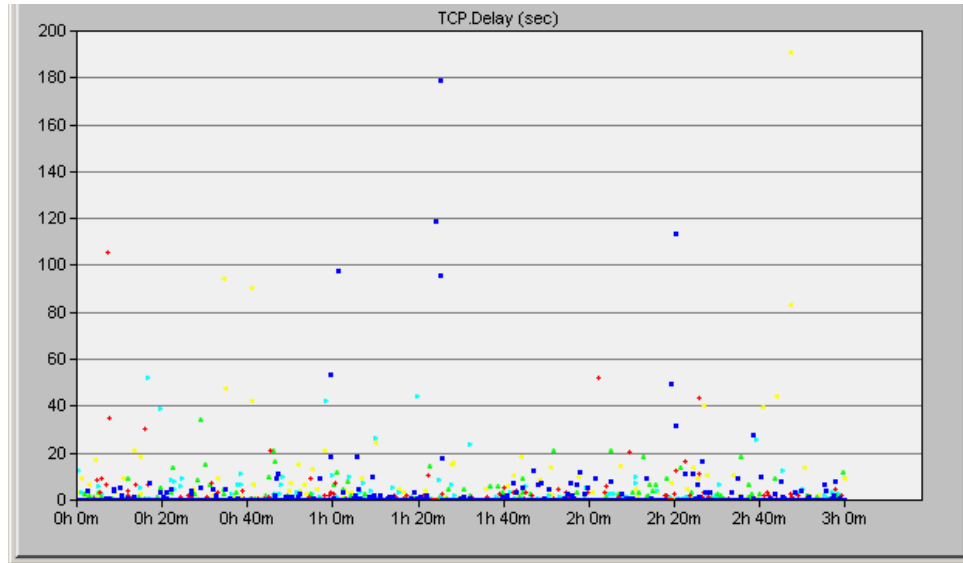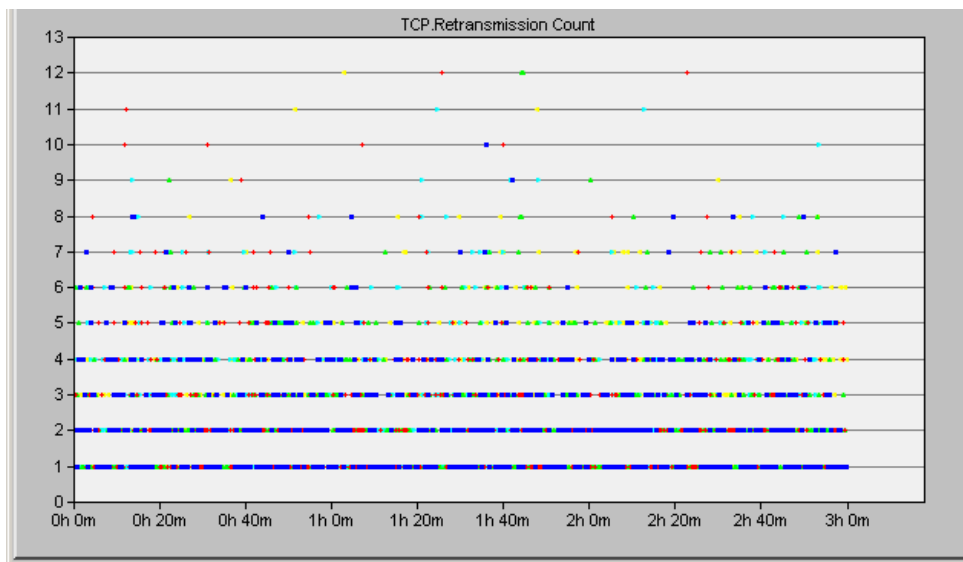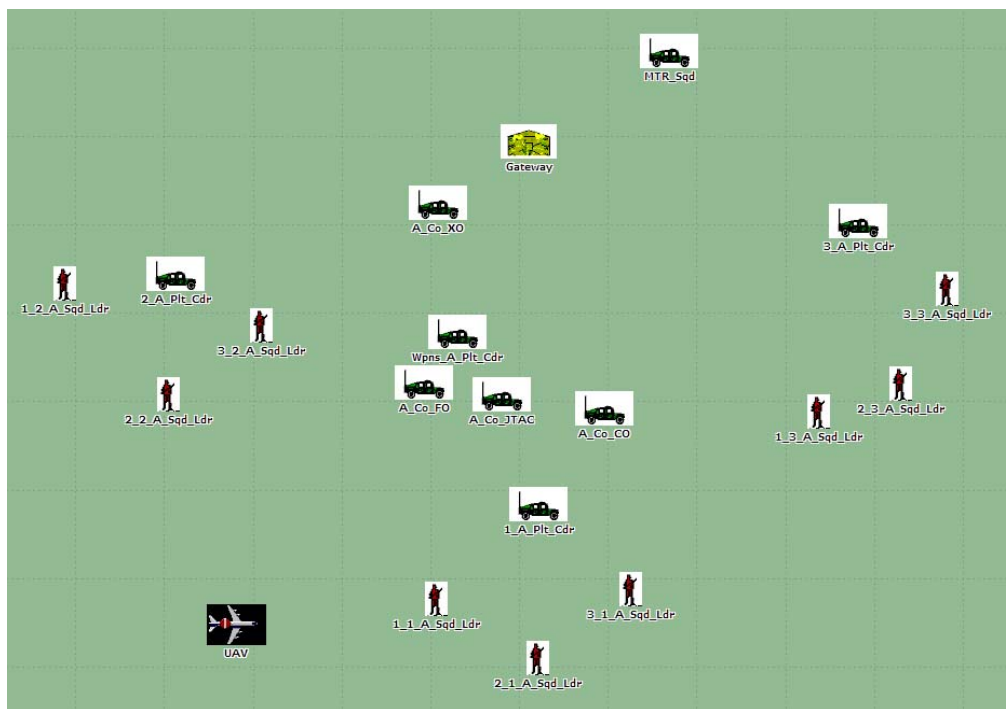

Figure 48.   Company Network Layout

Each node attached to the network is li mited to tran smitting the types of traffic allowed by the application profile associat ed with that particular node during   each scenario. Therefore, depe nding on the scenario, som e nodes m ay introduce different types and quantities of network traf fic than the other nodes. The applications associated with each node attempt to m imic the types of traffic that w ould be reas onably expected from the type of job assigned to each node.   A squad leader is only allowed to use the position update and short message applications; the mortar platoon, forward observer and JTAC can only use the position update, short message and fire support applications; and the platoon commander, XO and CO can use a ll application profiles. The gateway node does not initiate the use of any applications. It only acts as a source for stream ing video, a recipient of position report data and sour   ce of TCP application   traffic, for no des sending TCP traffic that is routed through the gateway.

1. Position Update Only

All three networks were ab le to support the application run in this sim ulation scenario. T he resu lts p resented in [1] show that the CDR network achieved a lo wer message delivery success rate of 95.0% during this scenario, and because it som etimes failed to deliver three to f our m essages in a row for various nodes, it was graded as a failing to support the app lication. We believe this criterio n to be somewhat harsh, since most tactical units will not have traveled a significant distance in a matter of only three or four m inutes. Those units that are travel ling f ast enough to re quire higher precision position location reporting are rarely not travel ling in groups, so while one node within the group may not be reporting current position information, the reports from other nodes associated with the sam e groups will m ore than make up for the lag in reporting from a single node. So, to be fair to the results shown in the CDR simulation, while we consider its support of the Position Update application in this scenario to be a success, we will upgrade it only to "Marginal" in our summary of results section at the end of this chapter. The SINCGARS network achieved a 100% message delivery success rate and the EPLRS network achieved a message delivery succes s rate of 97.62%. The results of the SINCGARS and EPLRS networks area presente d in greate r detail in the f ollowing two sections.

a. SINCGARS Results

The SINCGARS network dem onstrated the same results in the Com pany Position Update Only scenario as it did in the Position Update Only Platoon scenario. It achieved a 100% m essage delivery success rate , with a m aximum rec eive and transm it throughput of 624 bps, and average throughput s of around 300 bps. Once again, these results are not very surprising, because each of the messages were offset from each other and transmitted at a constant ra te, so with trans mission overlaps caus ed by variatio ns in transmission tim es, we expected there to be no transmission collisions. Potential collisions experienced in actual deploym ent of a SINCGARS i mplementation of s uch a

lightly-loaded network c ould be ea sily m itigated by an application lev el CSMA MAC protocol. The graphs f or this scenario l ook exactly the sam e as those for the Platoon scenario, so they are not included in this section.

b. EPLRS Results

The average EPLRS node transm ission throughput for this scenario was almost four tim es as high as the platoon ve rsion of this scenar io, and the average reception throughput was roughly eight tim es as high, as shown in Figures 49 and 50. It is in teresting to note that the S INCGARS network did not show the sam e overall throughput deviations from the platoon si mulations, and it achieved 100% m essage delivery, while the EPLRS network only ach ieved a 97.62% m essage delivery success rate. This is because each SINCGARS node m akes no attem pt to relay other no des' messages. This dem onstrates that the us e of a multi-hop n etwork in a scenario w here most nodes are with in one hop of each other m ay actually degrade overall network performance.
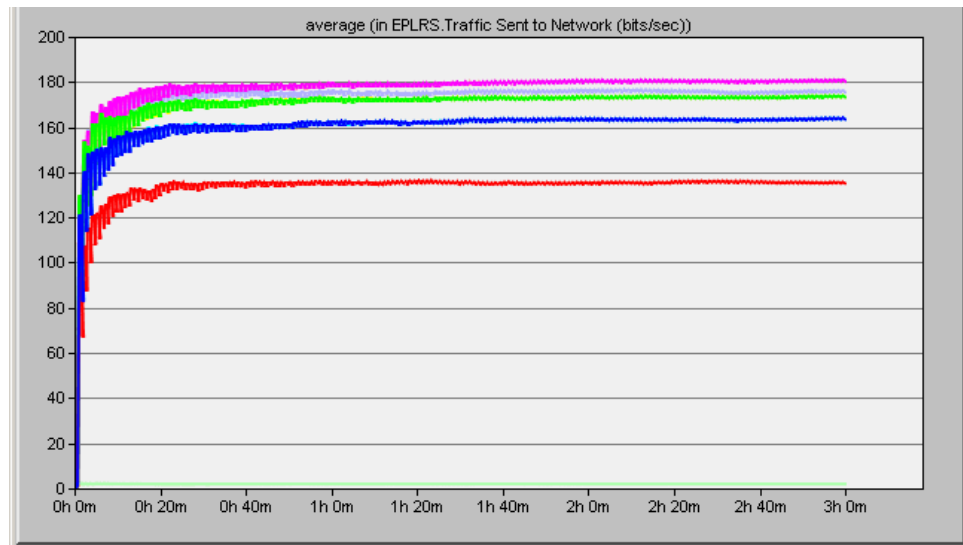

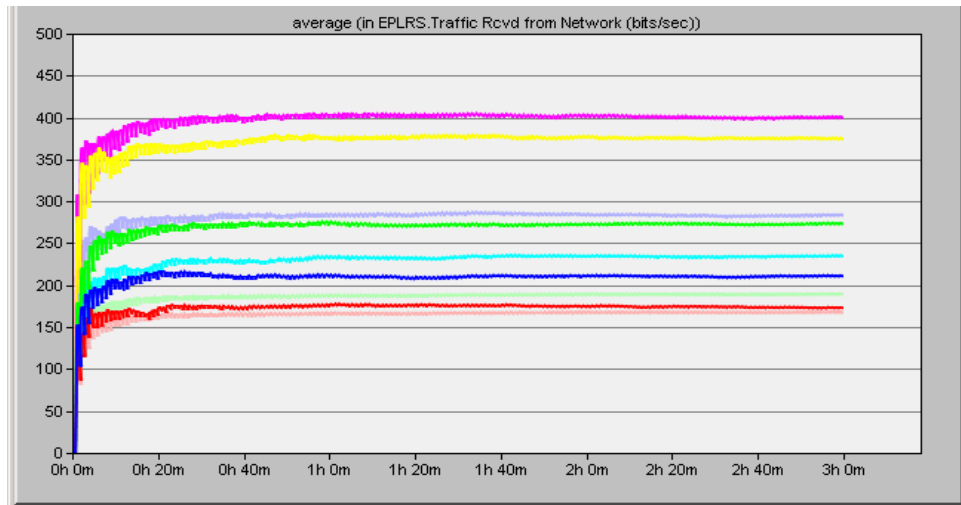Figure 49.   EPLRS Company (Position Update Only): Average Tx Throughput

Figure 50.   EPLRS Company (Position Update Only): Average Rx Throughput

2.   Short Message Only

The CDR achieved a 9 8.6% message delivery success rate, with an average TCP latency of 1.67 seconds.   This m essage com pletion rate is not considered accep table, since text messages are rarely sent in a tactical environment that do not contain important and usually som ewhat tim e sensitive comm unications. Since even a single m issed message could have significant im pact on operations, it m ay be prudent to augm ent the TCP acknowledgment for short message application messages with a protocol that forces an autom atic retran smission of failed messages. The SINCGARS achieved a m arginal 99.79% overall success rate and the EPLRS   network achiev ed a failing 55.47% overall success rate.   The results of the SINCGARS   and EPLRS networks area presented in greater detail in the following two sections.

a.   SINCGARS Results

The SINCGARS network achieved   a 99.79% m essage delivery success rate for the Short Message Only Company s cenario, only s lightly lower than the su ccess rate achieved during the platoon version of   the sam e scenario. Of the 7991 m essages delivered, o nly 17 failed to arriv e at th eir destination.   The peak reception   and transmission throughputs were 2880 bps, with an average throughput of around 280 bps.

86

The average node throughput graphs for this   scenario look the sam e as those for the Platoon scenario, so they are not included here.

Figure 51 shows how both the aver   age TCP delay and m aximum TCP delay showed only slight increases from the platoon version of this scenario, increasing from 0.772 and 2.082 seconds to 0.8625 and 3.4 s econds, respectively. T he average and peak TCP r etransmission counts increased from the platoon scenario, with an average retransmission count of 1.8077 (up fr   om 1.25), and a m   aximum count   of 9 retransmissions (up from only 2), as depicted in Figure 52, and is a result of the increased quantity of overall transmissions being broadcast across this network.
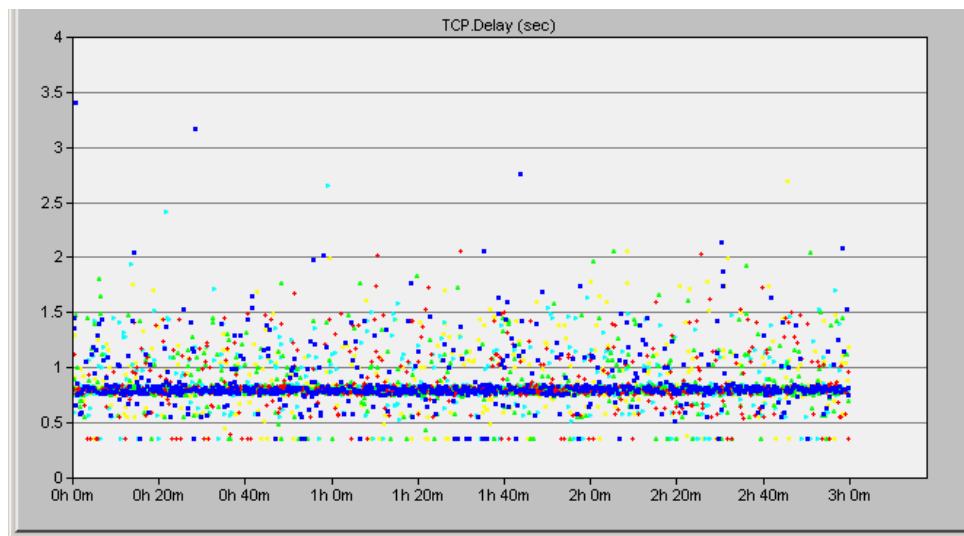

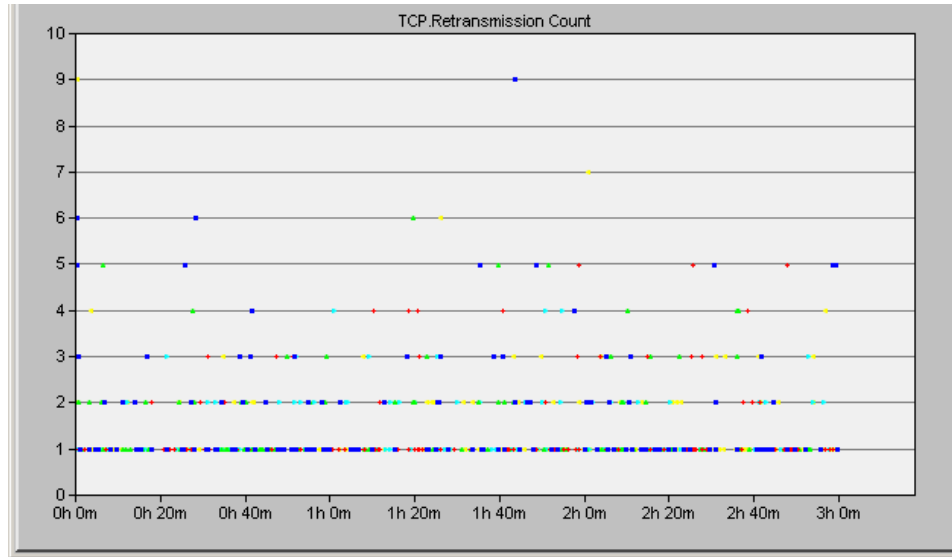Figure 51.　　　SINCGARS Company (Short Message Only): TCP Delay

Figure 52.   SINCGARS Company (Short Message Only): TCP Retransmission Count

b.   EPLRS Results

In Figures 53 and 54, we see that som e of the nodes closest to the m iddle of the netw ork (JTAC and CO nodes – top   two lines) both receiv e and transm it more traffic than those nodes that are further aw ay from the other nodes (MT R node – bottom line). This is because the nodes in the m   iddle of the network ar e attem pting to relay traffic from one side of the network to the ot   her, which is beneficial if the fringe nodes are not within transmission range of each othe r, but not when the relay s are unnecessary. We also notice that the am   ount of t ransmission and rece ption throughputs are roughly nine times greater here, than they were dur ing the platoon sim ulations runs, whereas the SINCGARS network showed alm ost no throughput increases. This further illustrates the significant increases in overall netw ork tra ffic experienced when using wireless multi-hop technologies, and should show why these t ypes of networks m ay not always be the most desirable configuration for every type of network lo ad. W hile multi-hop networks are intend ed to extend the reachability of m   obile (and fixed) nodes, the characteristics inherent to multi-hop transm issions can degr ade network p erformance if all nodes   are within transm ission range of each other. Un   less there is a way for gr oups of nodes to perceive th eir p roximity to   each   othe r an d dynam ically alter their m   ulti-hop

88

configurations, applications that function we ll when all nodes are spread out, m ay not perform as well when they become more tightly grouped.
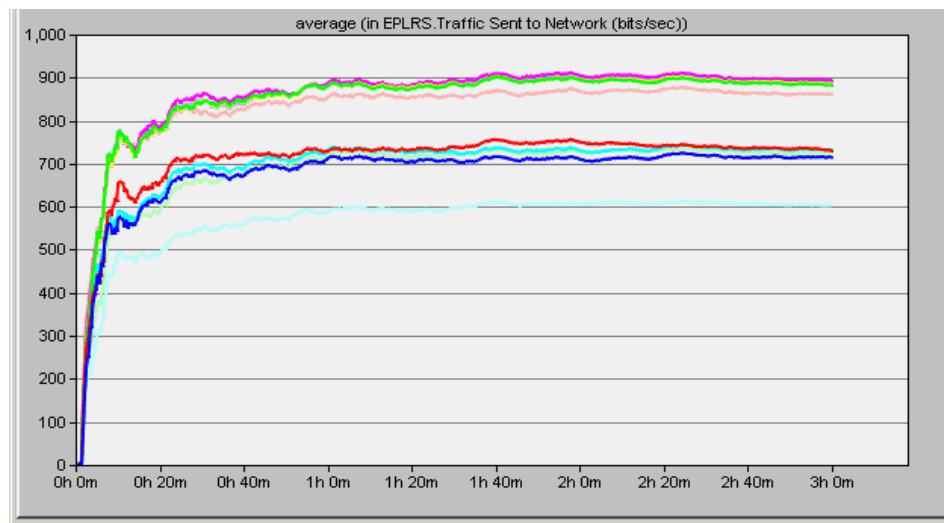

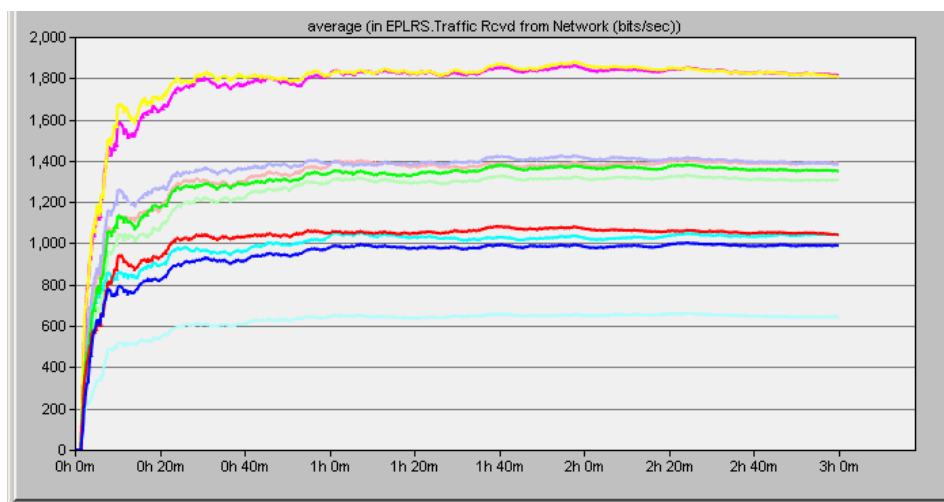Figure 53. EPLRS Company (Short Message Only): Average Tx Throughput

Figure 54. EPLRS Company (Short Message Only): Average Rx Throughput

Figure 55 shows that the average TCP Delay was 1.393 seconds, with a maximum delay of 92.3 seconds, which is si gnificantly greater than the 0.862 second average and 3.4 second peak TCP delays experienced by the SINCGARS network. As depicted in Figure 56, the average TCP retransmission count was 6.736, with a maximum of 25, which is m ore than double the retran smission counts experienced by the EP LRS network running the same applications on the platoon scenario.
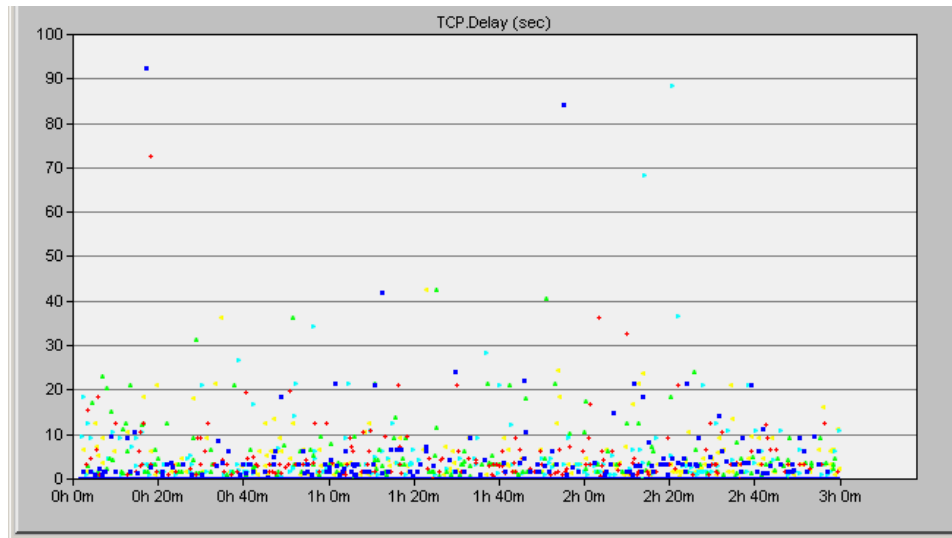
Figure 55.   EPLRS Company (Short Message Only): TCP Delay
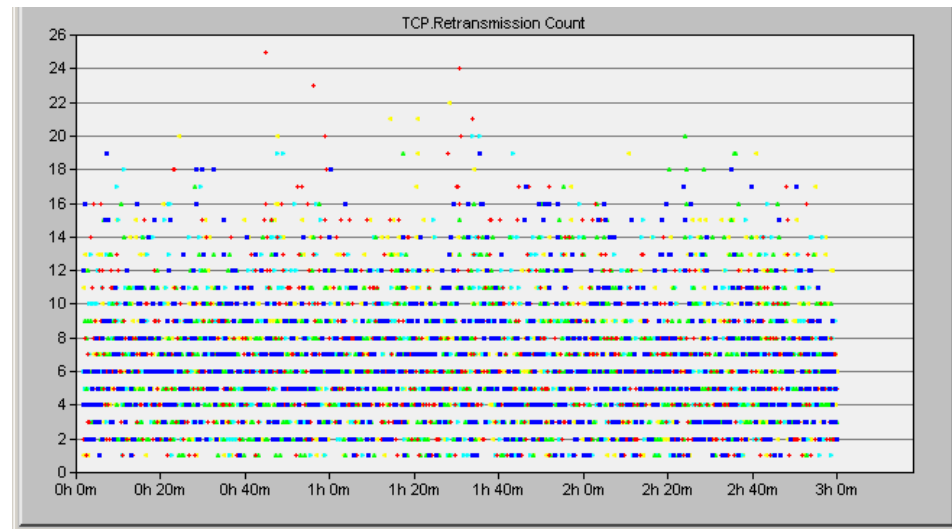
Figure 56.   EPLRS Company (Short Message Only): TCP Retransmission Count

3.   Commanders and Position

As explained in [1], the CDR simulation runs were only able to complete between 12-60 minutes of each 3 -hour simulation. No CDR network m essage completion rates were provided for this scenario, but it   was m entioned that the HTTP and Em   ail applications failed to deliver all of their application messages. The SINCGARS network achieved a 24.4% ov   erall m essage deliv ery success rate and the EPLRS network

achieved a 66.59% overall message delivery success rate. The results of the SINCGARS and EPLRS networks area presented in greater detail in the following two sections.

%	CDR	SINCGARS	EPLRS
Position Update	Not Available	100	0
Short Message	Not Available	92.77	66.49
IRC	Not Available	1.81	82.94
HTTP	0	82.65	93.33
Email	0	82.65	93.33

Table 7.   Commanders and Position Application Success Rates (Company)

a.   SINCGARS Results

The initial r un of this s imulation sc enario crashed after 1 hour and 49 minutes of sim ulation time, due to the JCSS program running out of m emory to allocate to support all of the sim ulation events. Conseq uently, we were only able to successfully complete five 1-hour simulations. Despite the reduced simulation tim e, enough data was collected to draw som e useful conclusions regarding the perfor mance of the SINCGARS network under the Commanders and Position simulation scenario.

The SINCGARS network achieved a si gnificantly lower overall m essage delivery success rate during this run than it   did during the platoon   version of the sam e scenario. Its overall m essage delivery success rate was only 24.4% for all transm issions generated during this scenario. This is not entirely surprising, since the higher number of nodes introducing traffic was expected to cause   a higher rate of tran smission collisions. The overall success rate seem s low when com pared to the individual application success rates, but since som e a pplications send si gnificantly m ore m essages than others, the overall message delivery success rate can be   impacted greatly by the failure of only the position update and IRC m essages, because these applicatio ns generate the m ost amount of network traffic. This sim   ulation r un illus trates how the non-CSMA MAC protocol being used with the SINCGARS networ   k does not perfor   m adequately under high network traffic load scenarios.

The peak reception and transmission throughputs were 12000 bps, with an average throughput generally around 300 bps . As show in Figure 57, the average reception th roughput was roughly half that of the sam e a pplication set run under the platoon scenario. This lower reception thro ughput is due to the increased am ounts of transmission collisions. If a tran smission is received and categorized as noise, it is not factored into the overall reception throughput ca lculations. The graphs for this scen ario look the same as those for the Platoon scenario, so they are not included here.
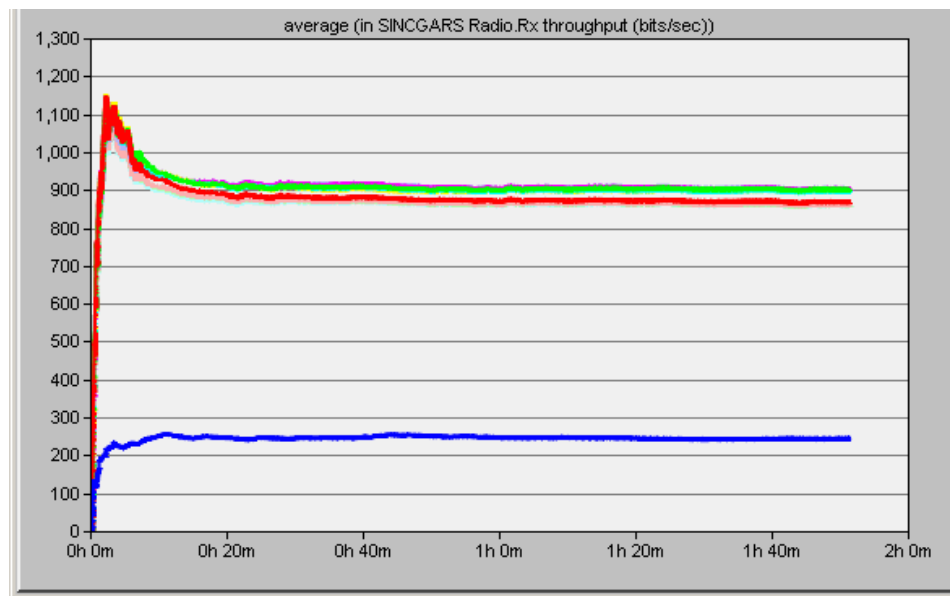

Figure 57.   SINCGARS Company (Commanders & Position): Average Rx Throughput

Figure 58 shows that both the av erage TCP delay and m aximum TCP delays shifted drastical ly from the platoon vers ion of this scenario, increasing from 1.12 and 11.1 seconds to 40.79 and 199.6 seconds, resp ectively. This is another significant illustration of how providing no q uality of se rvice for a h igher traf fic density ne twork will resu lt in extrem ely poor perform ance. The average and peak TCP retransm ission counts showed much less significant increases from the platoon scenario, with an average retransmission count of 1.867 (up from 1.12), and a m aximum count of 11 retransmissions (up from only 2), as depicted in Figure 59.
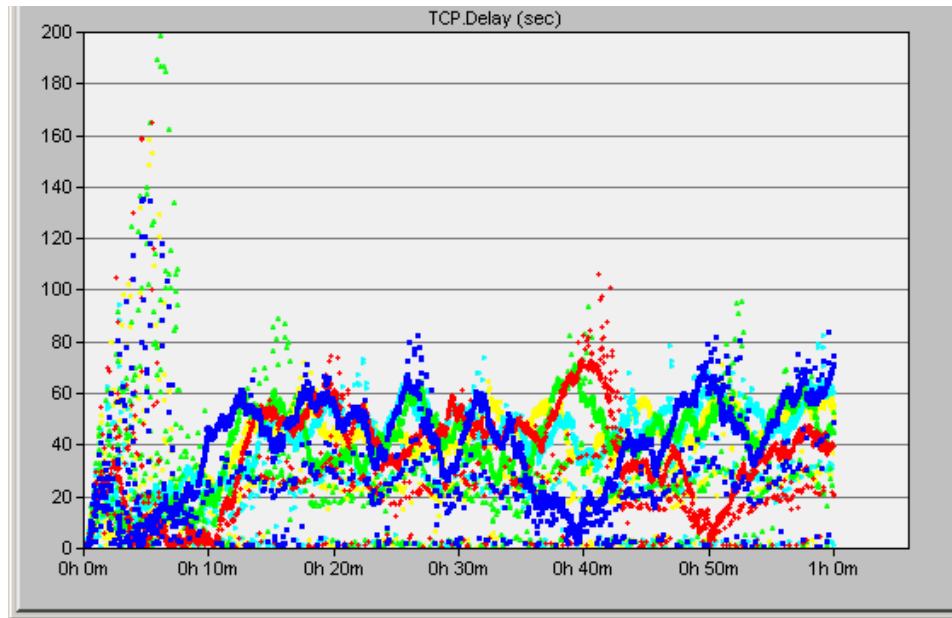
Figure 58.   SINCGARS Company (Commanders & Position): TCP Delay
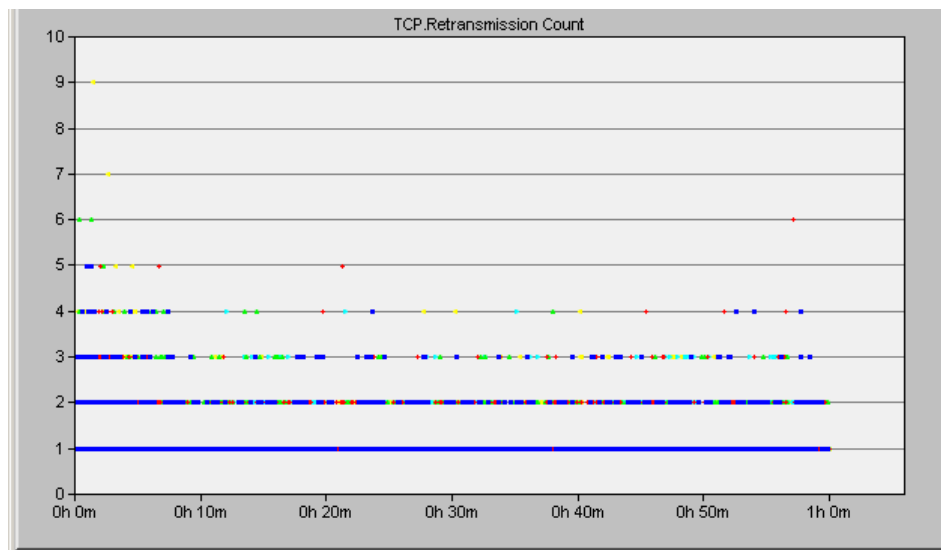
Figure 59.   SINCGARS Company (Commanders & Position): TCP Retransmission Count

b.   *EPLRS Results*

The EPLRS network achieved a significantly lower overall m   essage delivery success rate during this run than it   did during the platoon   version of the sam e scenario. T his is not entirely surprising,   since the higher num ber of nodes introducing traffic was expected to   cause a higher rate   of transm ission collisions. The EPLRS

achieved slightly better perform ance over the SINCGARS network f or this scena rio, which demonstrates the CSMA node's advantage over a non-CSMA node for busier networks.

Figures 60 and 61 show that the av erage transm ission and recep tion throughputs are enormously larger than bo th the com pany-sized comm anders and position SINCGARS t hroughputs, and the pl atoon-sized comm anders and position EPLRS throughputs (as m uch as 40 tim es larger for some nodes). This increase in throughput is caused by both the increase in traffic from there being more nodes initiating traffic, and more relaying transmissions associated with each additional node.
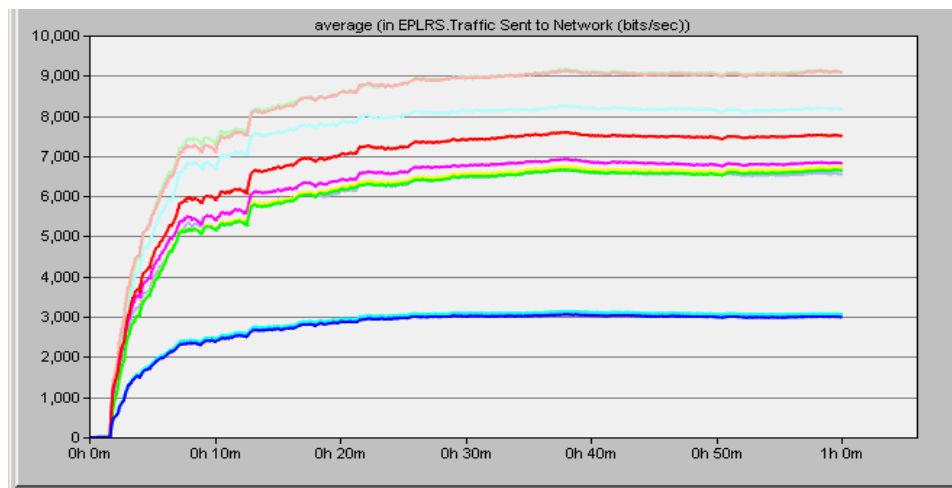

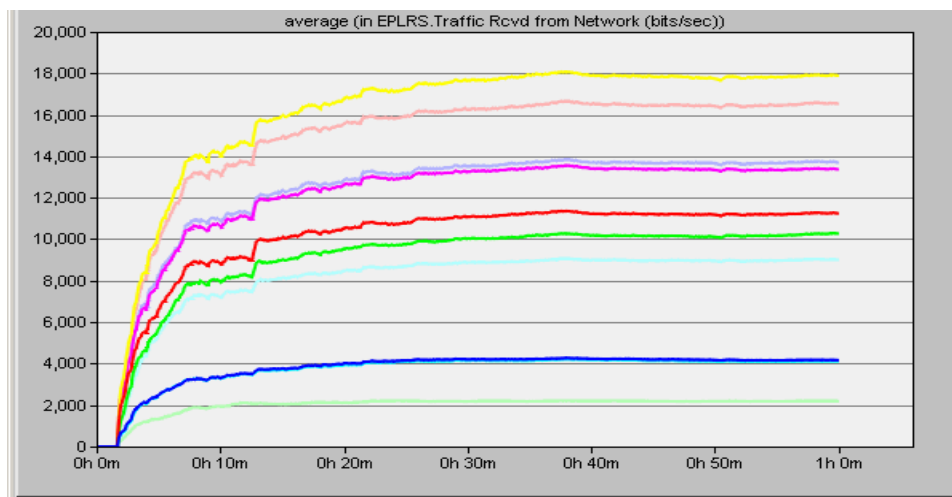Figure 60.   EPLRS Company (Commanders & Position): Average Tx Throughput

Figure 61.   EPLRS Company (Commanders & Position): Average Rx Throughput

Figure 62 shows that both the av erage TCP delay and m aximum TCP delays increased from the platoon version of this scenario, increasing from 2.24 a nd 15 seconds to 2.66 and 433.6 seconds, respectively. This is another significant illustration of how greatly message relaying can affect the performance network. The average and peak TCP retransmission counts showed much less significant shifts from the platoon scenario, with an average retransm ission count of 4.143 (up from 2.24), and a m aximum count of 15 retransmissions (down from 21), as depicted in Figure 63.
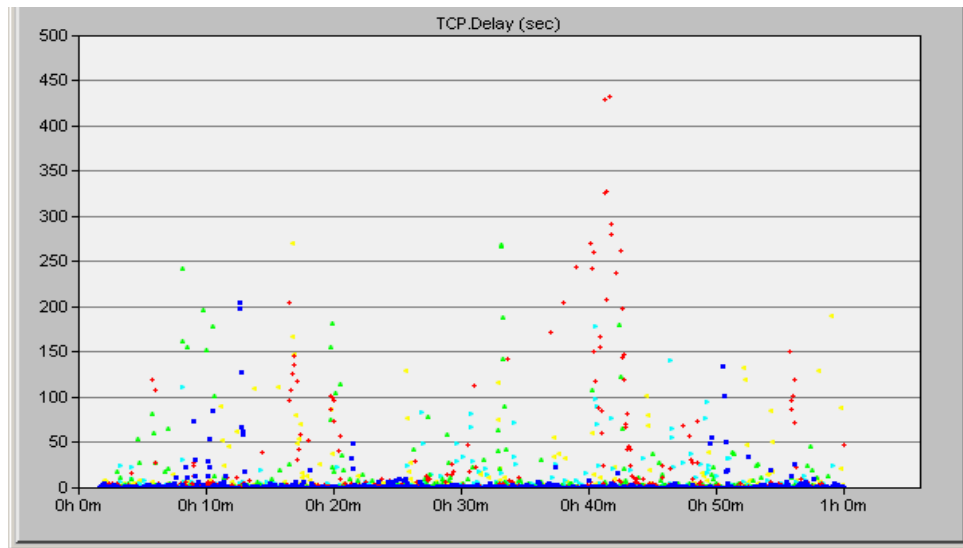

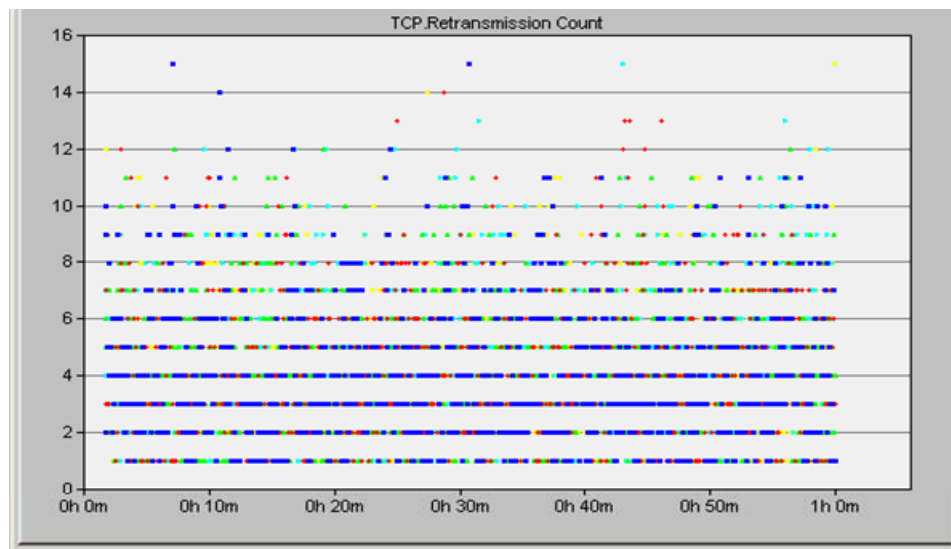Figure 62.   EPLRS Company (Commanders & Position): TCP Delay

Figure 63.   EPLRS Company (Commanders & Position): TCP Retransmission Count

D.   SUMMARY OF RESULTS

Our networ k sim ulation resu lts f or th e SINCGARS and EPLRS radio networks are presented in Tables 8 and 9. We have   categorized each radio's perf ormance in each scenario as achieving one of three levels of   support: Successful, Marginal, and Failure. The Position Update application is graded less strictly, as the nature of these applications allow for greater tolerance of undelivered   messages, and the Short Message and Email applications are graded more   strictly, since the failure to deliver one of these m essages can result in much more serious con sequences. Since th e Video application rep resented an already poor quality video   feed of two fram es per sec ond, a network's inability to provide near 100% support to this resulted in a failing grade. If a network cannot support this degraded version of our Video applica   tion, then it would certainly not be able to support the greater demands of a regular quality video feed.

CDR (Platoon)

	Position Update Only	Short Msg Only	Cdr & Pos	Current	All
Position Update	SUCCESS		SUCCESS	SUCCESS	SUCCESS
Short Message		MARGINAL	SUCCESS	MARGINAL	MARGINAL
IRC			SUCCESS		SUCCESS
HTTP			MARGINAL		FAILURE
Email			MARGINAL		FAILURE
Video				MARGINAL	MARGINAL

SINCGARS (Platoon)

	Position Update Only	Short Msg Only	Cdr & Pos	Current	All
Position Update	SUCCESS		SUCCESS	SUCCESS	FAILURE
Short Message		MARGINAL	MARGINAL	FAILURE	FAILURE
IRC			SUCCESS		FAILURE
HTTP			SUCCESS		FAILURE
Email			SUCCESS		FAILURE
Video				FAILURE	FAILURE

EPLRS (Platoon)

	Position Update Only	Short Msg Only	Cdr & Pos	Current	All
Position Update	SUCCESS		SUCCESS	FAILURE	FAILURE
Short Message		FAILURE	FAILURE	FAILURE	FAILURE
IRC			FAILURE		MARGINAL
HTTP			MARGINAL		MARGINAL
Email			MARGINAL		MARGINAL
Video				MARGINAL	FAILURE

Table 8.   Network Simulation Results (Platoon)

CDR (Company)					
	Position Update Only	Short Msg Only	Cdr & Pos	Current	All
Position Update	MARGINAL		FAILURE	N/A	N/A
Short Message		FAILURE	FAILURE	N/A	N/A
IRC			FAILURE		N/A
HTTP			FAILURE		N/A
Email			FAILURE		N/A
Video				N/A	N/A
SINCGARS (Company)					
	Position Update Only	Short Msg Only	Cdr & Pos	Current	All
Position Update	SUCCESS		SUCCESS	N/A	N/A
Short Message		MARGINAL	FAILURE	N/A	N/A
IRC			FAILURE		N/A
HTTP			FAILURE		N/A
Email			FAILURE		N/A
Video				N/A	N/A
EPLRS (Company)					
	Position Update Only	Short Msg Only	Cdr & Pos	Current	All
Position Update	MARGINAL		FAILURE	N/A	N/A
Short Message		FAILURE	FAILURE	N/A	N/A
IRC			FAILURE		N/A
HTTP			MARGINAL		N/A
Email			MARGINAL		N/A
Video				N/A	N/A

Table 9.   Network Simulation Results (Platoon)

From these results, we can conclu   de th at under very light network loads, the SINCGARS radio network, with its ALOHA-like MAC protoc ol, performed better under lighter network loads, but as   the amount of network traffi c increased, its perform ance quickly deteriorated.

In light of its occas   ionally better pe rformance for some of our simulation scenarios, it is worth pointing out th   at the S INCGARS does not support m   ulti-hop networks. Since these scenarios only presented application traffic generated by stationary entities that were all within   a single hop of each other, th   ese results do not accurately reflect this radio' s inab ility to sup port the se s ame application req uirements to mobile users who travel further than one hop away from any traffic-generating node.

Across the entire set of our network simulations, the EPLRS device was only able to support 2 of the 23 application instances su ccessfully. It is worth noting that, while this device does support up to 32 sim ultaneously separated channels (or needlines), we chose to have all applications in each of our simulations share the same channel, in order to provide a m ore accurate basis for com parison of the p erformance of a sing le EPLRS needline to the other two radios. Sin ce the CDR simulations in [1] attempted to supp ort all of its applications using only a single channel, and the SINCGARS only supports the use of one c hannel at a tim e, we chose to model the EPLRS perform ance across a single needline, as well. Even with the greater throughput capabilities of the EPLRS device, the addition of the TCP ove rhead proved to be too great for this m ulti-hop device to su pport with its CSMA needlin e. These r esults do no t reflect the E PLRS device's overall ability to support data applications in general, but m erely demonstrate the performance characteristic differences inherent to each type of wireless ne twork technology across a single channel.

The dism al results of our EPLRS node's use of TCP traffic de monstrates the potentially negative effects of using TCP- like protocols across m ulti-hop networks. When mobile multi-hop network nod es transition from being spread ou t to being within close proxim ity to each other, the increased traffic load of TCP-like protocols and the subsequent transm ission relays of each of thes e additional transm issions can p resent performance degradations that hamper e ffective network support of tactical data applications. Our results imply that a multi-hop network implementation that assumes all nodes within a given network will maintain some degree of separation, and does not have a well-defined transmission relay policy, m ay not effectively support the requirem ents of tactical mobile data networks.

Our simulation results also dem onstrate how th e use of coo perative div ersity by the CDR multi-hop network, when com pared to the EPLRS m ulti-hop network th at did not use cooperative div ersity, effectively m itigated some of the effects of the m ulti-path conditions caused by m essage relaying in the smaller network scenarios, but was unable to effectively m itigate the sam e conditions for larger netw orks. This dem onstrates that the use of cooperative diversity alone m ay not be able to overcom e the increased

transmission load for multi-hop n   etworks that are tem   porarily operating in   close proximity to a large number of other multi-hop nodes belonging to the same network.

We m ust also point out that none of thes   e sim ulations included the effects that tactical voice comm unications m ay have on creating additional network delays. While the EPLRS may be able to provide non-conflic ting support for tactical voice applications with the imple   mentation of a VoIP-only   data needline, the   addition of voice communication dem ands to the S INCGARS netw ork would alm ost certainly prevent it from achieving the sa   me level of success it   had in our sim   ulations, since all data communications would be blocked during the transmission of voice network traffic.

Additionally, these app   lication p rofiles may not reflect exact parameters of similarly named applications running across ac tual deployed system s. These application parameters were m   erely used to provide   reasonable comparisons to the previously determined CDR sim ulation resu lts, to show com   parable SINCGARS and EPLRS network performances under like network loads, and our results are not intended to im ply that actual applications with similar names or purposes will perform at the same levels on the devices mentioned in this th esis. Refining the application profiles to more accurately match the characteristics of actually deployed applications will be left for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

VI.   CONCLUSIONS AND FUTURE RESEARCH

A.   CONCLUSIONS

With the su dden growth in the d evelopment of m ore efficient and more capab le wireless communication technologies, it is no   surprise that there are m   any pote ntially useful military applications for most of these communication advances. The m ilitary has always relied on its   ability to harn ess the newest typ es of technology to enhance th e effectiveness of its command and control arch itecture, yet much of its currently deployed tactical co mmunication equipm ent predate ev en the widespread us e of the Internet. Adaptations to these older radios have been   periodically introduced, in an   effort to temporarily close the gap between the olde   r technologies and newer ones, but rarely arrive in the form of acceptable long-term technology solutions.

Newer devices have been fielded, but   none of these new er devices has been capable of com pletely replacing our older equi pment. As a result, we have a comm and and control architecture that is com posed of many different types of networking devices that perform very specific f unctions very well, but are in capable of com municating with each other. W ith our increased d emand and dependence on these newer data networking technologies, the consolidation of comm unication capabilities into a sm aller arsenal of more advanced networking devices is im   perative to the continued im provement of our tactical networking architecture.

In this the   sis we recr eated the n etwork simulation sc   enarios used f or the evaluation of an exper imental cooperative   diversity-based radio   (CDR), analyzed in previous th esis work [1]. We used thes   e sam e scenario s to evaluate comm unication devices that are cur rently in use by the m ilitary, and quantify the ac tual level of inability of these d evices to p rovide the type of com bined communi cation capab ilities n eeded in our present day tactical environm   ent. W e subjected each device to   the sam e sets of network tr affic loads as the CDR, in order   to d emonstrate the actual measured sh ift in performance that this one new technol   ogy provides over the older communication devices. Even though the CDR im plements one relatively new wi reless technology, both

101

the SINCGARS and the EPLRS ne tworks occasionally outperformed the CDR network with their older technologies. The primary take-away from our simulation results is that the technology being used for a particular type of communication network must match the needs of the network. If it does not do this, then overall network performance may be significantly degraded, regardless of how new or exciting the implemented technology. We saw that under lightly trafficked networks, the more complicated technologies failed to perform at the same high levels as the more simple technologies. However, as the scenarios increased their traffic load, the more complicated devices began to show more superior performance levels than the more simple communication devices.

Our simulation results illustrate some of the problems encountered when using different types of wireless networking technologies to support a variety of tactical network traffic scenarios, especially when multi-hop configurations are used in scenarios where it is not needed. We demonstrated that when all multi-hop network nodes are operating within a single hop of each other (a scenario that would not be uncommon for mobile tactical nodes), without a well-defined transmission routing or forwarding policies, these multi-hop technologies actually degrade overall network performance. Additionally, the only advantage of the cooperative diversity capability of the CDR is in its ability to simultaneously relay a single common frame by multiple sources, which implicitly requires a true multi-hop, or at least a multi-path environment to prove beneficial and also does not significantly benefit the performance of these mobile multi-hop networks under close node proximity situations. Therefore, we see that while certain emerging wireless technologies may solve connectivity issues involving communication between distant nodes, they introduce new challenges for ensuring continued communication between non-distant nodes belonging to the same network. While no one technology is going to solve all of the problems encountered in the employment of wireless mobile communication devices, the combination of the right technologies may effectively mitigate many of these issues.

B. FUTURE WORK

1. Tactical Network Application Refinement

The applications used in our JCSS sim ulations were rec reated to m imic those presented in [1], in order to create an accu rate basis of comparison for both the SINCGARS and EPLRS to the perform ances of the CDR Actual characteristics of applications running in current tactical environm ent m ay va ry from those presented in this evaluation. The collection and validati on of actual application statistics and the subsequent transform ation of these statisti cs into JCSS application profiles could be immensely beneficial to future JCSS evaluatio ns of tactical communication technologies, as a ready-made framework for consistent software evaluation of tactical mobile wireless devices is not currently available through OPNET or JCSS network simulation suites.

2. Wireless Mobile Device Benchmark Criteria

The com bination of a s tandard se t o f JCSS/OPNET device applic ations with a n extensive set of realistic ev aluation scenarios could be us ed as a m uch more thorou gh benchmarking method for the com parison of cu rrently deployed devices to experim ental devices, th an the scen arios presented in this thesis. Establishing device software simulation benchm arking criteria would not only present a consistent m ethod of identifying the strengths and weaknesses of various communication devices, it would present potential vendors with a comprehensive se t of criteria needed to create an "ideal radio" device for various types of applicati ons (i.e., a device that could achieve 100 % message delivery success rate during each of the benchmark scenarios). This would have to be a large and varied set of scenarios, including sim ulated node trajectories, terrain modeling and various types of non-node signal interferences (environmental and hostile).

3. JCSS Scenario Refinement for Currently Deployed Devices

The creation of more complex JCSS simulation scenarios for the SINCGARS and the EPLRS would provide additional baseli ne com parisons for the evaluation of emerging wireless technologies. T hese sim ulations could com bine larger networks of

mobile nodes that actually travel along various types and com binations of node trajectories, or com bine different nodes with a variety of device configurations (i.e., changing needline type for an EPLRS network). This would provide useful insight into the actual capabilities and limitations of currently deployed comm unication devices, and would provide m ore effective baselines for further com parisons between these dev ices and experimental ones.

4. SINCGARS Mobile Ad Hoc Application JCSS Evaluation

Previous thesis research [6] provided an experim ental imple mentation of an application that created MANETs usi ng SINCGARS radios. Creating an OPNET Modeler model for this application, and then evaluating its perform ance under a variety of network sim ulation scenarios would be us eful in discussing the perfor mance of this application on a larger scale, and could be us ed to m ake comparisons to other emerging MANET technologies.

5. Multi-hop Network Protocol Analysis and Refinement

As new m obile wireless networking tec hnologies continue to develop, it m ay be possible to redefine both older MA C and m essage exchange protocols to m ake more efficient use of the new technologies within a tactical environment. As dem onstrated in this thesis, the increased transm ission lo ad of TCP-like protoc ols can introduce enough overhead to significantly degrade the perform ance of m ulti-hop netwo rks, when most nodes in th e network are within a single hop of each other. Protoco ls that allo w for dynamic multi-hop configuration alterations, based on proxim ity to other nodes in the network could allow greater efficiency for ne tworks where mobile users operate across a wide range of proxim ity to other nodes in the network. A m ethodical performance evaluation and com parison of existing wireless networking protocols with protocols that have been suggested but not yet im plemented, using network sim ulation software woul d provide valuable quantification of actua l improvem ents or degradations caused by implementing one protocol over another.

LIST OF REFERENCES

[1]   Byron R. Harder, *Analytical and Simulation-Based Assessment of a Prototype Tactical Multi-Hop Radio Network*, Naval Postgraduate School, September 2008.

[2] Lang   Tong, Wireless *Ad-Hoc Networks with Receiver Multipacket Reception*, Army Research Office, September 2004.

[3] Dr.   Bhaskar Krishnamachari, *Scalability Analysis of the TrellisWare Approach to Ad Hoc Wireless Networking*, University of Southern California, April 2007.

[4]   Adam Blair, Thomas Brown, Keith M. Chugg, Mark Johnson, *Tactical Mobile Mesh Network System Design*, TrellisWare Technologies, Inc. and University of Southern California, June 2008.

[5]   *OPNET Modeler 14.5 Product Documentation,* OPNET Technologies, Inc., Bethesda, MD © 1987-2008.

[6]   Steven Brand, A *Software-Based Network Infrastructure For Mobile Ad Hoc Data Networking In Support Of Small Tactical Units Using the SINCGARS Radio*, Master's Thesis, Naval Postgraduate School, March 2006.

[7]   *Planner's Manual for EPLRS Networks*, TB 11-5825-298-10-3, ENM Software Version 4.4, EPLRS Radio Software Version 11.4, Headquarters, Department of the Army, August 15, 2004.

[8]   *SINCGARS ICOM Ground Radios*, TM 11-5820-890-10-6, Headquarters, Department of the Army, August 1, 1998.

[9]   J. Nicholas Laneman, David N. C. Tse, Gregory W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, December 2004.

[10]   Robert D. Martin, Dr. Harlan B. Russell, *Investigation of Least Resistance Routing in a Mobile SINCGARS Packet Radio Network*, Clemson University and Techno-Sciences Inc., 1996.

[11]   *TALK-II SINCGARS: Multiservice Communications Procedures for the Single Channel Ground and Airborne Radio System*, FM 11-1, Air Land Sea Application Center, May 1996.

[12]   *Enhanced Position Location Reporting System (EPLRS) Model User's Guide*, OPNET Technologies, Inc., Bethesda, MD © January 7, 2008.

[13]   *TACTICAL RADIOS: Multiservice Communications Procedures for Tactical Radios in a Joint Environment*, FM 6-02.72, Air Land Sea Application Center, June 2002.

[14]   James F. Kurose, Keith W. Ross, *Computer Networking: A Top-Down Approach, 4th Edition*, Addison Wesley Publishing, Boston, 2008.

[15] John   Viega, *Practical Random Number Generation in Software*, Virginia Tech, Annual Computer Security Applications Conference, 2003.

[16]   K. Pawlikowski, Joshua Jeong, Ruth Lee, "On Credibility of Simulation Studies of Telecommunication Networks," *IEEE Communications Magazine*, vol. 40, no. 1, January 2002, pp 132-139.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (ATTN: Operations Officer)
   Camp Pendleton, California

7. Professor John Gibson
   Naval Postgraduate School
   Monterey, California